US006594764B1

(12) **United States Patent**
Wishner et al.

(10) **Patent No.: US 6,594,764 B1**
(45) **Date of Patent: Jul. 15, 2003**

(54) **APPARATUS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR NETWORK MANAGEMENT OPERATIONS RELATING TO NETWORK MANAGEMENT PROTOCOL ADAPTER SECURITY SOFTWARE (MPASS) FOR MESSAGING WITH USER NAME ACCESS IDENTIFICATION**

(75) Inventors: **Josie Anne Wishner**, Seattle, WA (US); **Balaji V. Pagadala**, Sunnyvale, CA (US); **Rajeev Angal**, Santa Clara, CA (US); **Subodh Bapat**, Palo Alto, CA (US)

(73) Assignee: **Sun Microsystems, Inc.**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/330,521**

(22) Filed: **Jun. 11, 1999**

(51) **Int. Cl.**[7] **G06F 9/00**

(52) **U.S. Cl.** **713/202**; 713/150; 713/153; 713/163; 713/168

(58) **Field of Search** 713/150, 153, 713/161, 163, 168, 182, 202

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,699,513 A * 12/1997 Feigen et al. 713/200

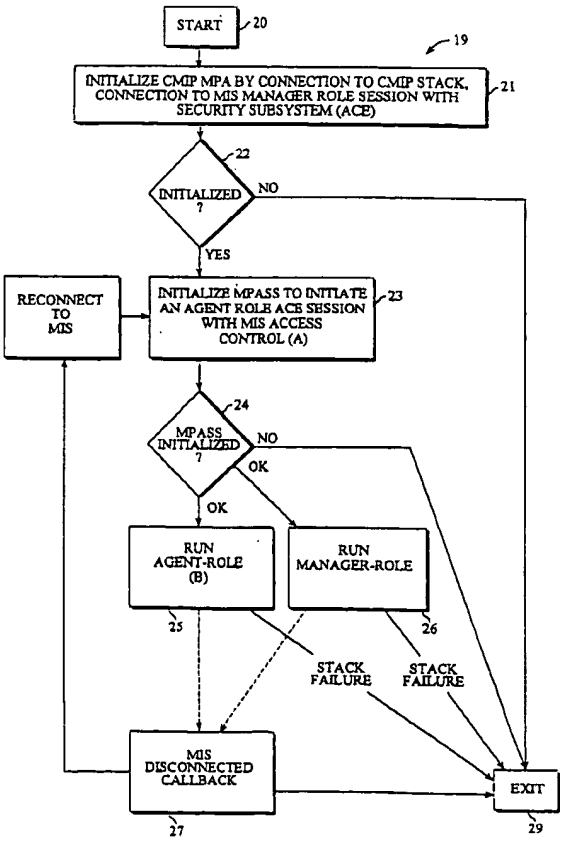
* cited by examiner

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Meyertons Hood Kivlin Kowert & Goetzel, P.C.; B. Noël Kivlin; Rory D. Rankin

(57) **ABSTRACT**

A computer implemented method and a computer program product includes a first computer readable code construct configured to handle request messages. This comprises receiving a request message and having an associated user name which is associated with a remote user on a network. Further, making an access determination to determine whether the forwarding of the request message is authorized, and finally when forwarding of the request message is authorized, the message to a target system is forwarded.

22 Claims, 13 Drawing Sheets



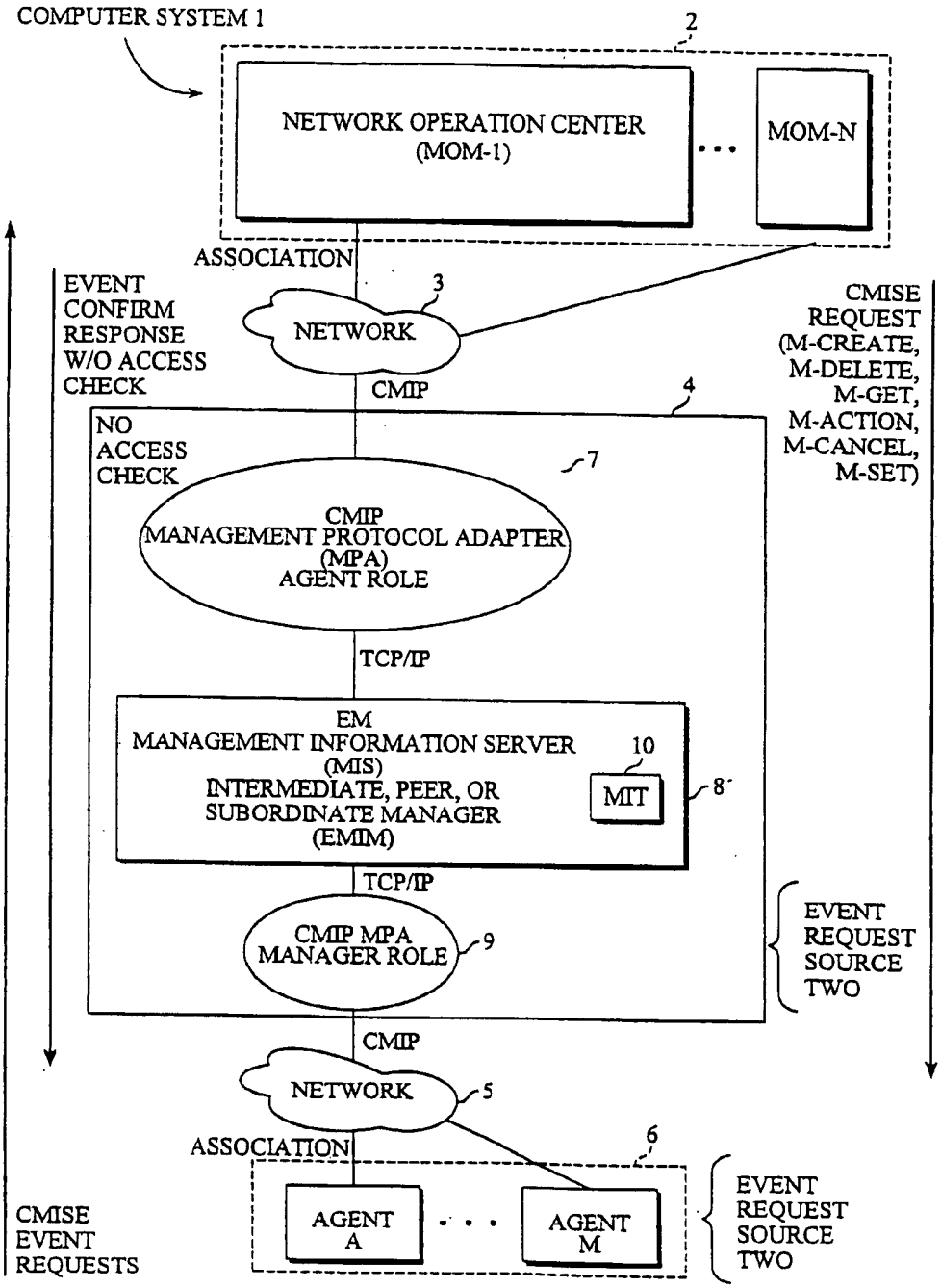

COMPUTER SYSTEM 1
2
NETWORK OPERATION CENTER (MOM-1)
MOM-N
ASSOCIATION
EVENT CONFIRM RESPONSE W/O ACCESS CHECK
3
NETWORK
CMIP
4
CMISE REQUEST (M-CREATE, M-DELETE, M-GET, M-ACTION, M-CANCEL, M-SET)
NO ACCESS CHECK
7
CMIP MANAGEMENT PROTOCOL ADAPTER (MPA) AGENT ROLE
TCP/IP
EM MANAGEMENT INFORMATION SERVER (MIS) INTERMEDIATE, PEER, OR SUBORDINATE MANAGER (EMIM)
10
MIT
8
TCP/IP
CMIP MPA MANAGER ROLE
9
EVENT REQUEST SOURCE TWO
CMIP
NETWORK
5
ASSOCIATION
6
AGENT A
AGENT M
EVENT REQUEST SOURCE TWO
CMISE EVENT REQUESTS

Fig. 1

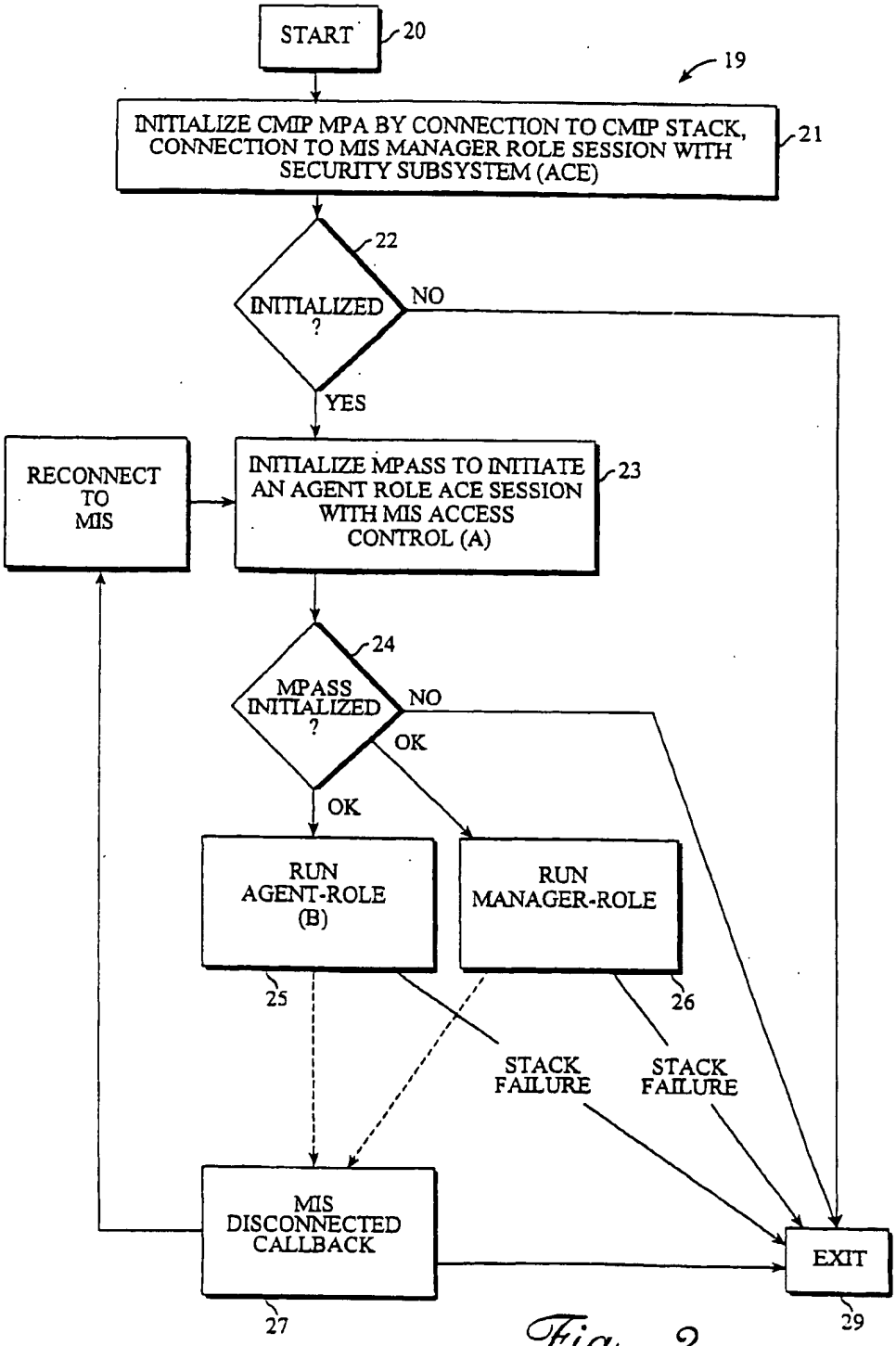

START
20
19
INITIALIZE CMIP MPA BY CONNECTION TO CMIP STACK, CONNECTION TO MIS MANAGER ROLE SESSION WITH SECURITY SUBSYSTEM (ACE)
21
22
INITIALIZED ?
NO
YES
RECONNECT TO MIS
INITIALIZE MPASS TO INITIATE AN AGENT ROLE ACE SESSION WITH MIS ACCESS CONTROL (A)
23
24
MPASS INITIALIZED ?
NO
OK
OK
RUN AGENT-ROLE (B)
RUN MANAGER-ROLE
25
26
STACK FAILURE
STACK FAILURE
MIS DISCONNECTED CALLBACK
EXIT
27
29

Fig. 2

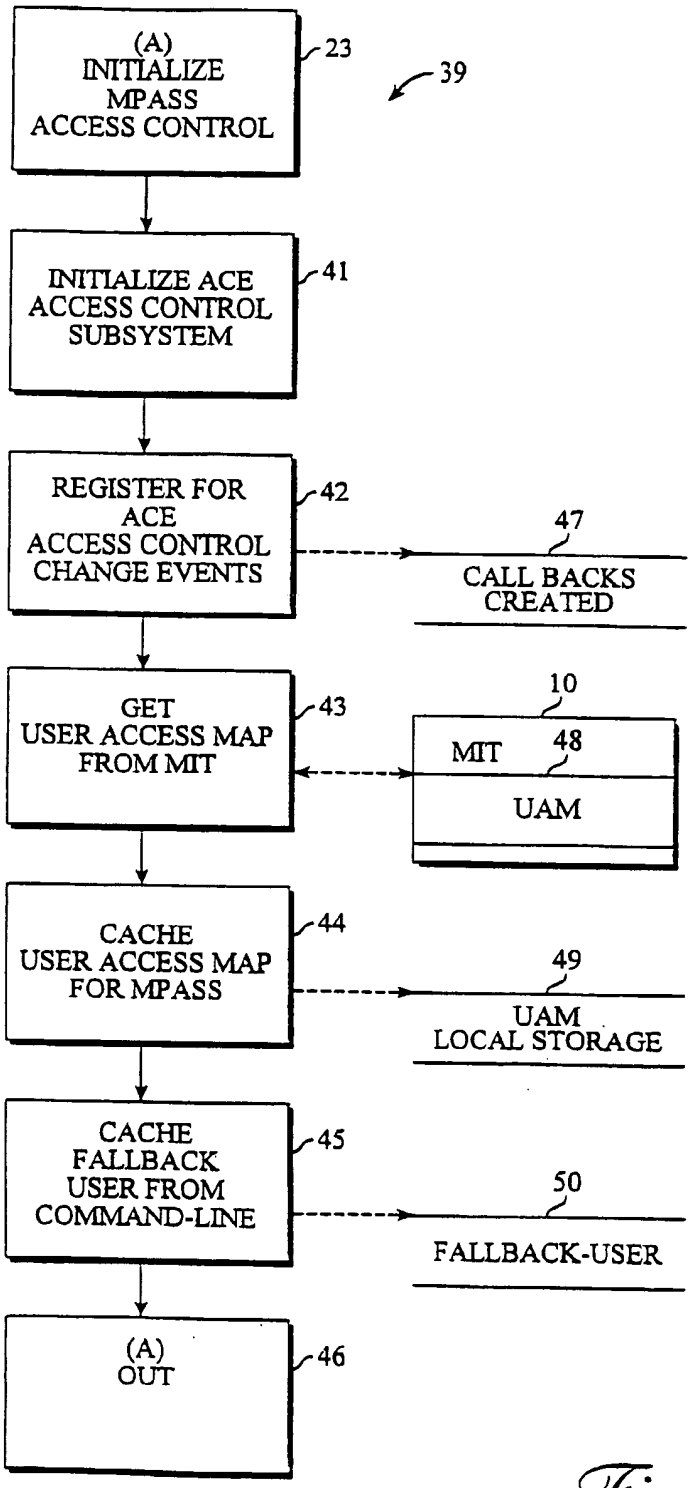

(A)
INITIALIZE
MPASS
ACCESS CONTROL
23
39
INITIALIZE ACE
ACCESS CONTROL
SUBSYSTEM
41
REGISTER FOR
ACE
ACCESS CONTROL
CHANGE EVENTS
42
47
CALL BACKS
CREATED
GET
USER ACCESS MAP
FROM MIT
43
10
MIT
48
UAM
CACHE
USER ACCESS MAP
FOR MPASS
44
49
UAM
LOCAL STORAGE
CACHE
FALLBACK
USER FROM
COMMAND-LINE
45
50
FALLBACK-USER
(A)
OUT
46

Fig. 3

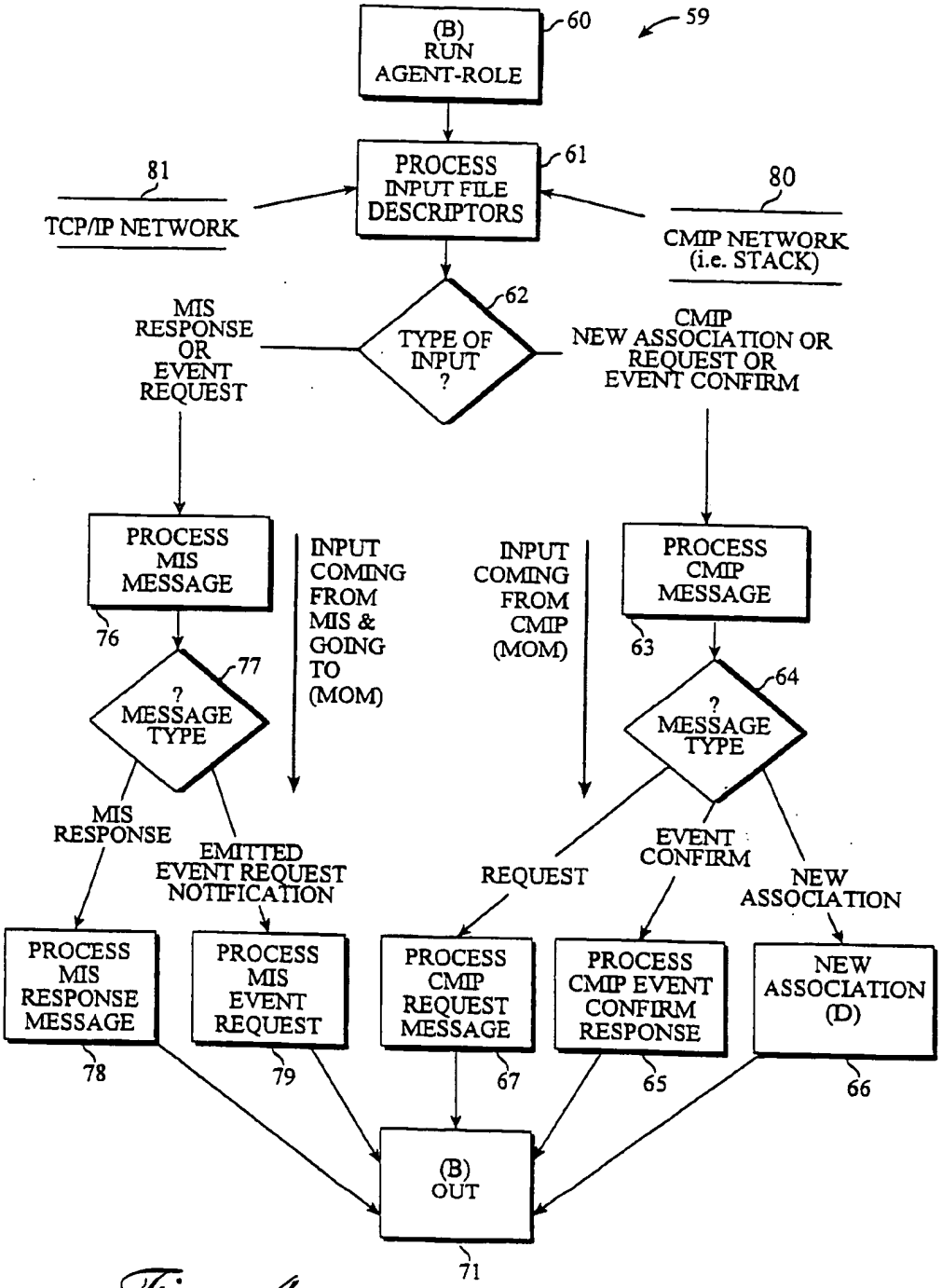

(B)
RUN
AGENT-ROLE
60
59
PROCESS
INPUT FILE
DESCRIPTORS
61
81
TCP/IP NETWORK
80
CMIP NETWORK
(i.e. STACK)
62
TYPE OF
INPUT
?
MIS
RESPONSE
OR
EVENT
REQUEST
CMIP
NEW ASSOCIATION OR
REQUEST OR
EVENT CONFIRM
PROCESS
MIS
MESSAGE
76
INPUT
COMING
FROM
MIS &
GOING
TO
(MOM)
INPUT
COMING
FROM
CMIP
(MOM)
PROCESS
CMIP
MESSAGE
63
77
?
MESSAGE
TYPE
64
?
MESSAGE
TYPE
MIS
RESPONSE
EMITTED
EVENT REQUEST
NOTIFICATION
REQUEST
EVENT
CONFIRM
NEW
ASSOCIATION
PROCESS
MIS
RESPONSE
MESSAGE
78
PROCESS
MIS
EVENT
REQUEST
79
PROCESS
CMIP
REQUEST
MESSAGE
67
PROCESS
CMIP EVENT
CONFIRM
RESPONSE
65
NEW
ASSOCIATION
(D)
66
(B)
OUT
71

Fig. 4

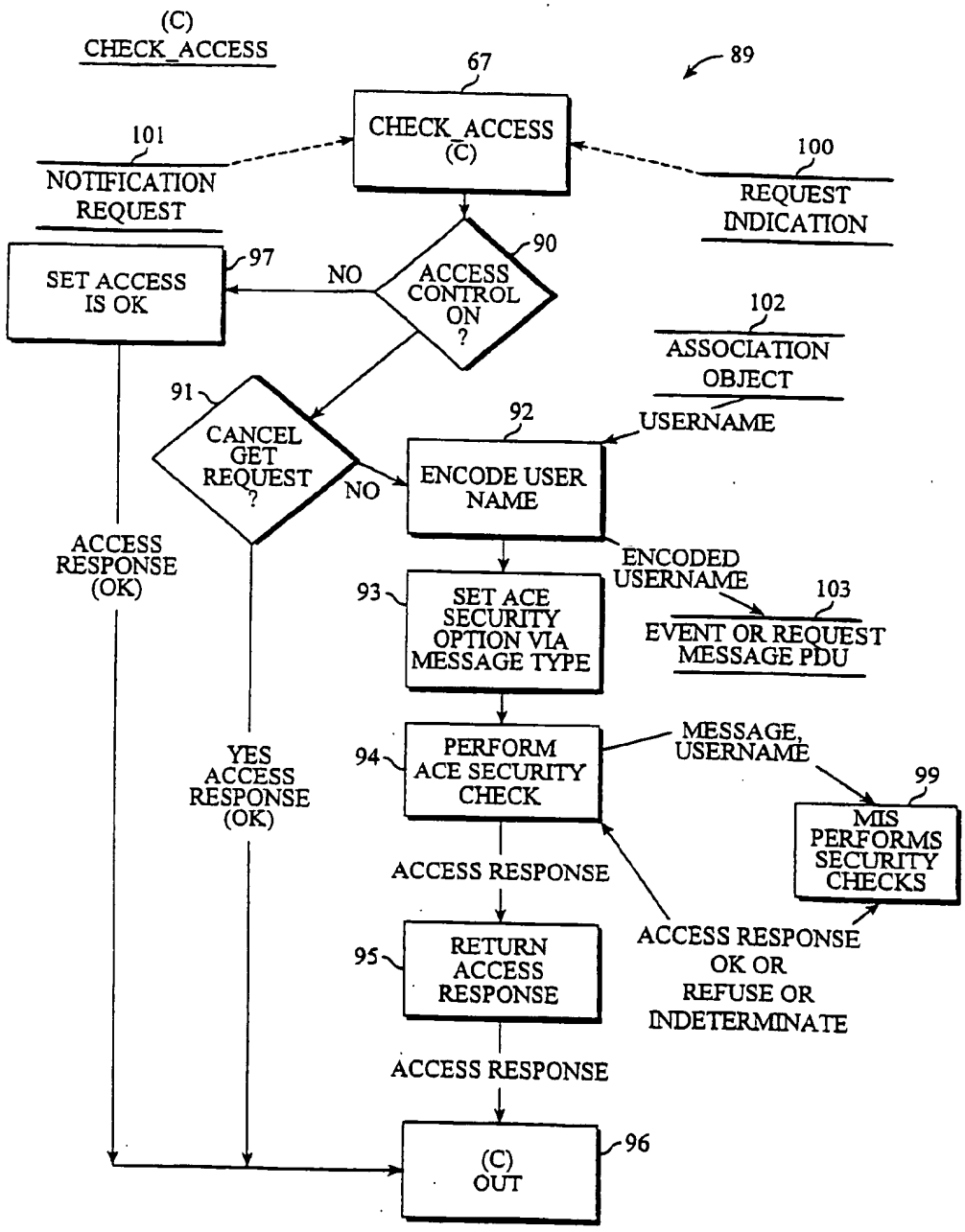

(C)
CHECK_ACCESS
67
89
CHECK_ACCESS
(C)
101
NOTIFICATION
REQUEST
100
REQUEST
INDICATION
SET ACCESS
IS OK
97
NO
ACCESS
CONTROL
ON
?
90
102
ASSOCIATION
OBJECT
91
CANCEL
GET
REQUEST
?
92
USERNAME
NO
ENCODE USER
NAME
ACCESS
RESPONSE
(OK)
ENCODED
USERNAME
93
SET ACE
SECURITY
OPTION VIA
MESSAGE TYPE
103
EVENT OR REQUEST
MESSAGE PDU
YES
ACCESS
RESPONSE
(OK)
94
PERFORM
ACE SECURITY
CHECK
MESSAGE,
USERNAME
99
MIS
PERFORMS
SECURITY
CHECKS
ACCESS RESPONSE
95
RETURN
ACCESS
RESPONSE
ACCESS RESPONSE
OK OR
REFUSE OR
INDETERMINATE
ACCESS RESPONSE
96
(C)
OUT

Fig. 5

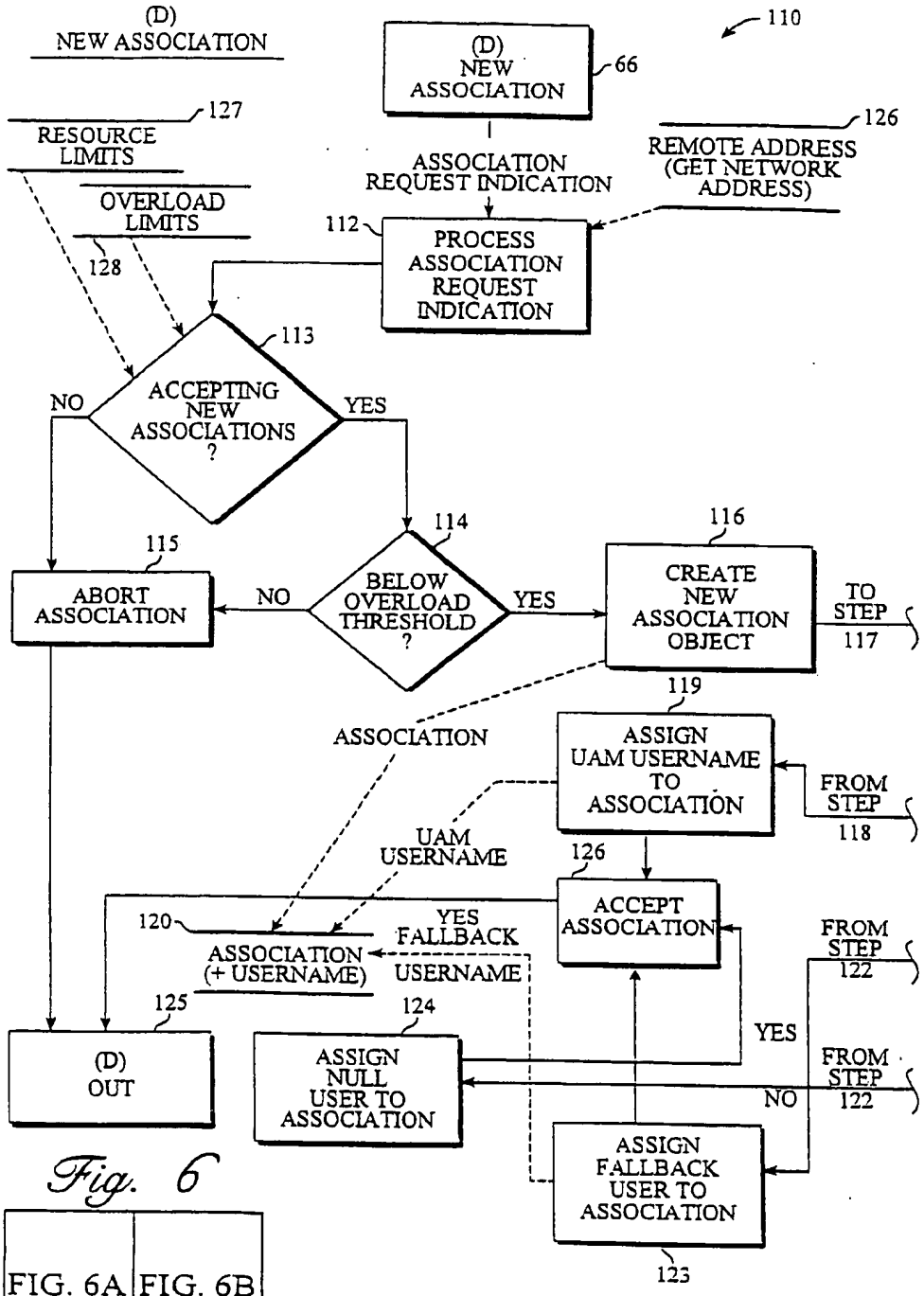


Fig. 6

FIG. 6A | FIG. 6B

Fig. 6A

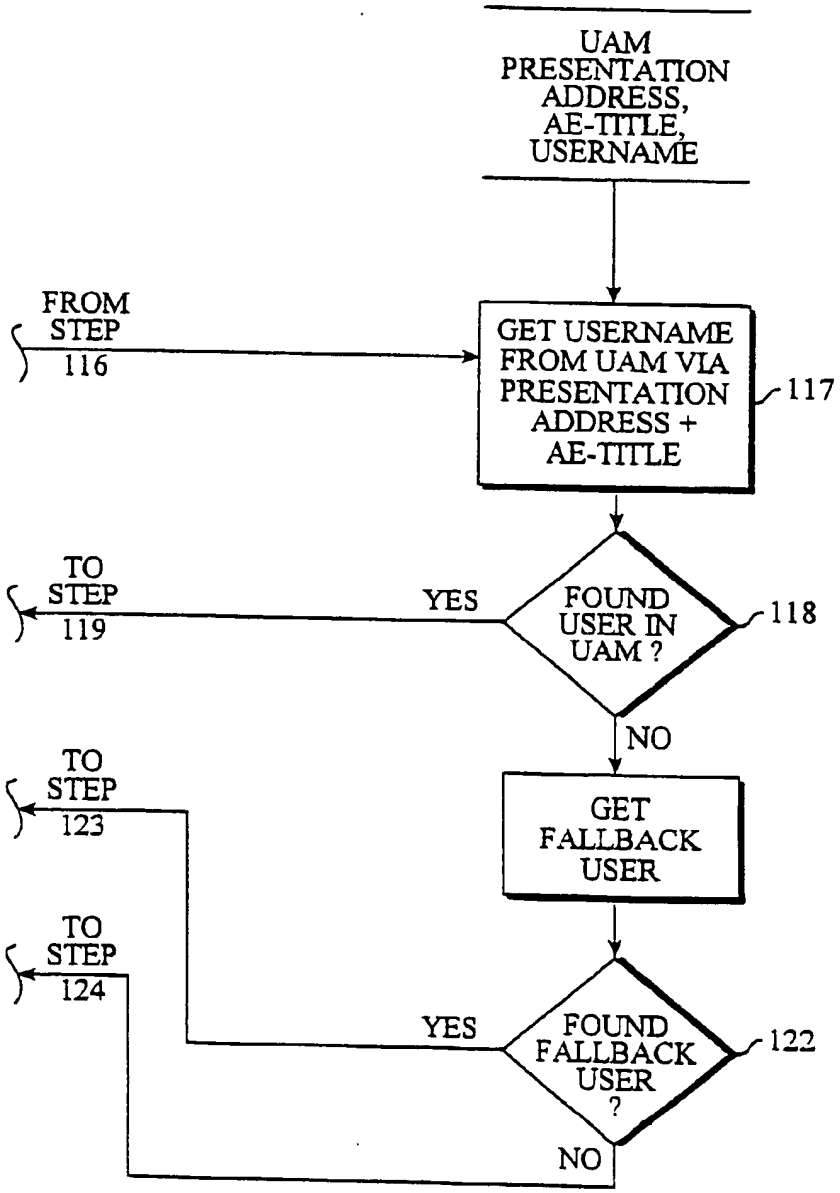

UAM PRESENTATION ADDRESS, AE-TITLE, USERNAME
FROM STEP 116
GET USERNAME FROM UAM VIA PRESENTATION ADDRESS + AE-TITLE
117
TO STEP 119
YES
FOUND USER IN UAM ?
118
NO
TO STEP 123
GET FALLBACK USER
TO STEP 124
YES
FOUND FALLBACK USER ?
122
NO

Fig. 6B

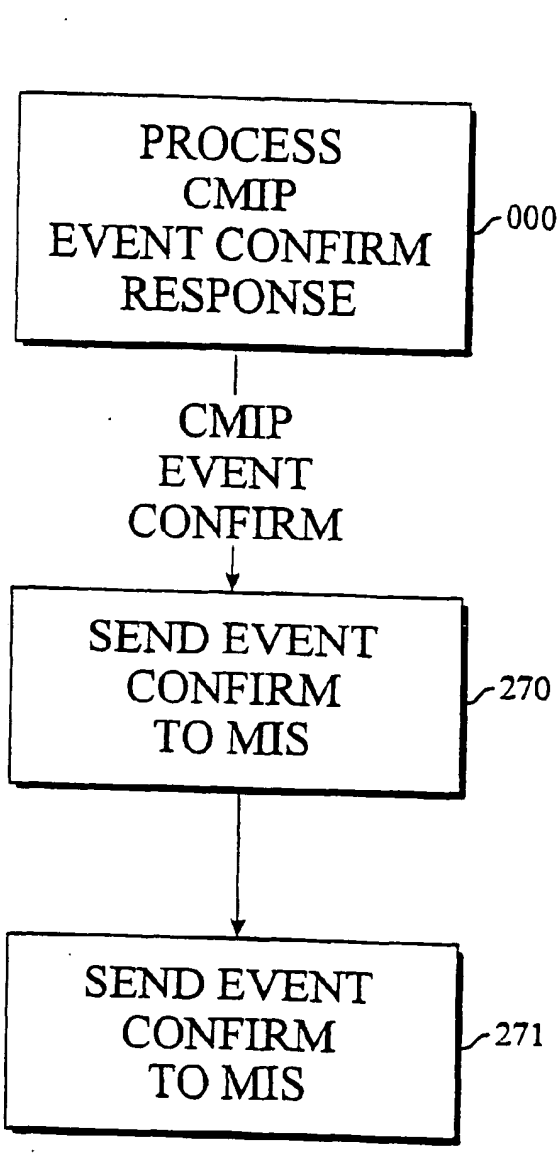

65
PROCESS CMIP EVENT CONFIRM RESPONSE
000
CMIP EVENT CONFIRM
SEND EVENT CONFIRM TO MIS
270
SEND EVENT CONFIRM TO MIS
271

Fig. 7

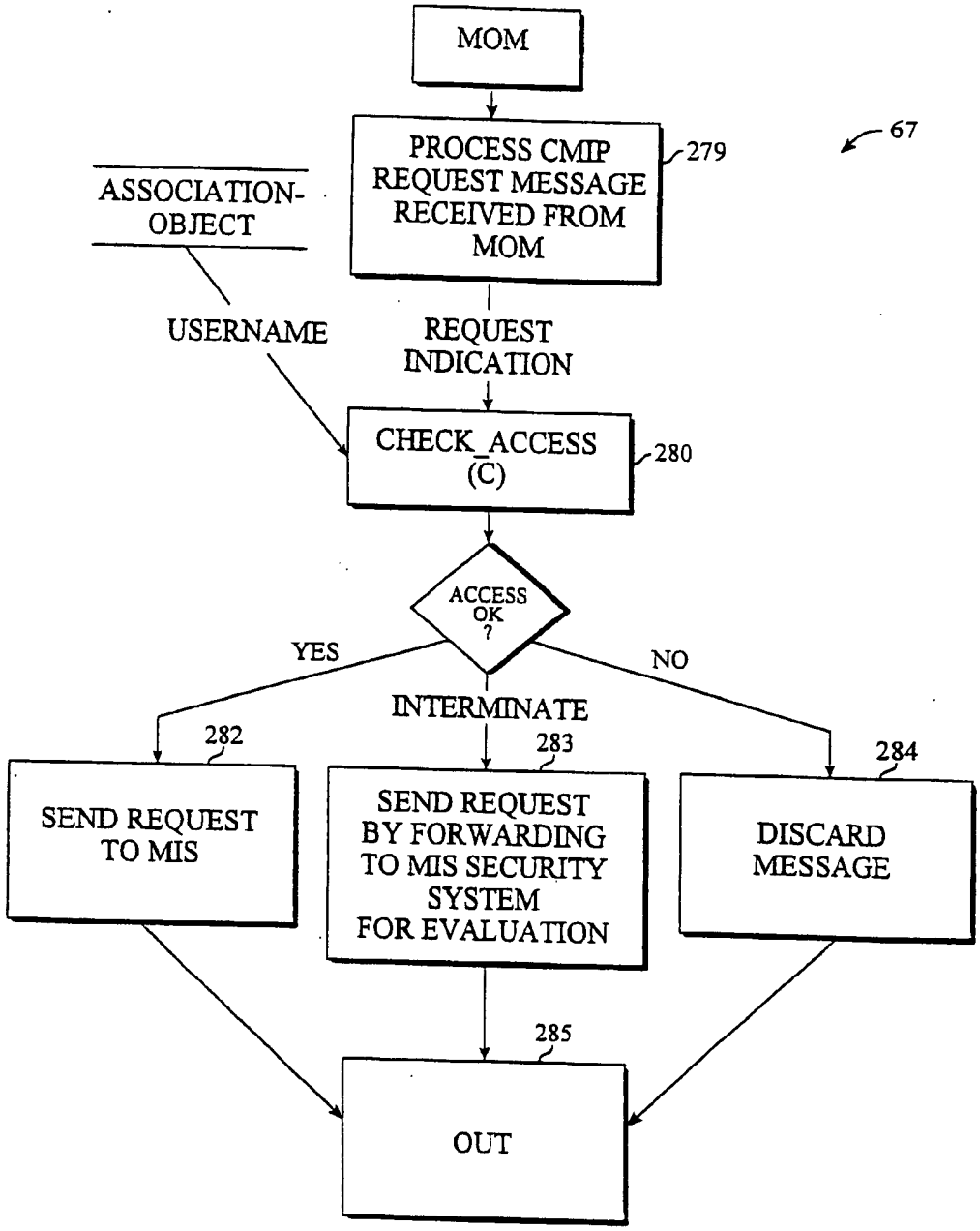

MOM
PROCESS CMIP REQUEST MESSAGE RECEIVED FROM MOM
279
67
ASSOCIATION-OBJECT
USERNAME
REQUEST INDICATION
CHECK_ACCESS (C)
280
ACCESS OK ?
YES
NO
INTERMINATE
282
283
284
SEND REQUEST TO MIS
SEND REQUEST BY FORWARDING TO MIS SECURITY SYSTEM FOR EVALUATION
DISCARD MESSAGE
285
OUT

Fig. 8

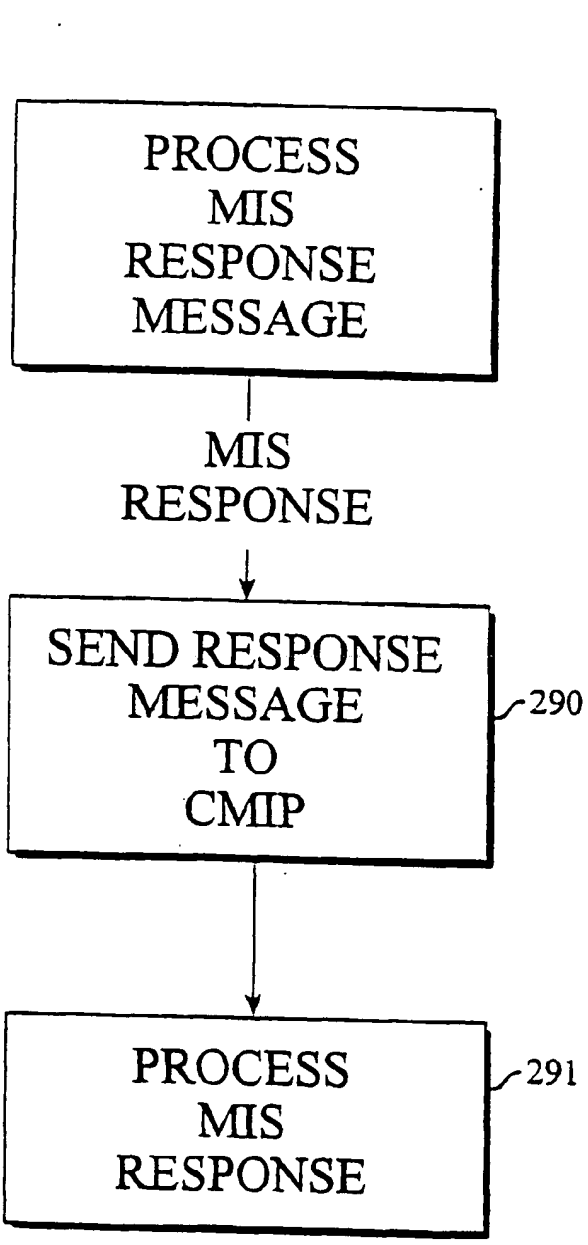

78
PROCESS MIS RESPONSE MESSAGE
MIS RESPONSE
SEND RESPONSE MESSAGE TO CMIP
290
PROCESS MIS RESPONSE
291

Fig. 9

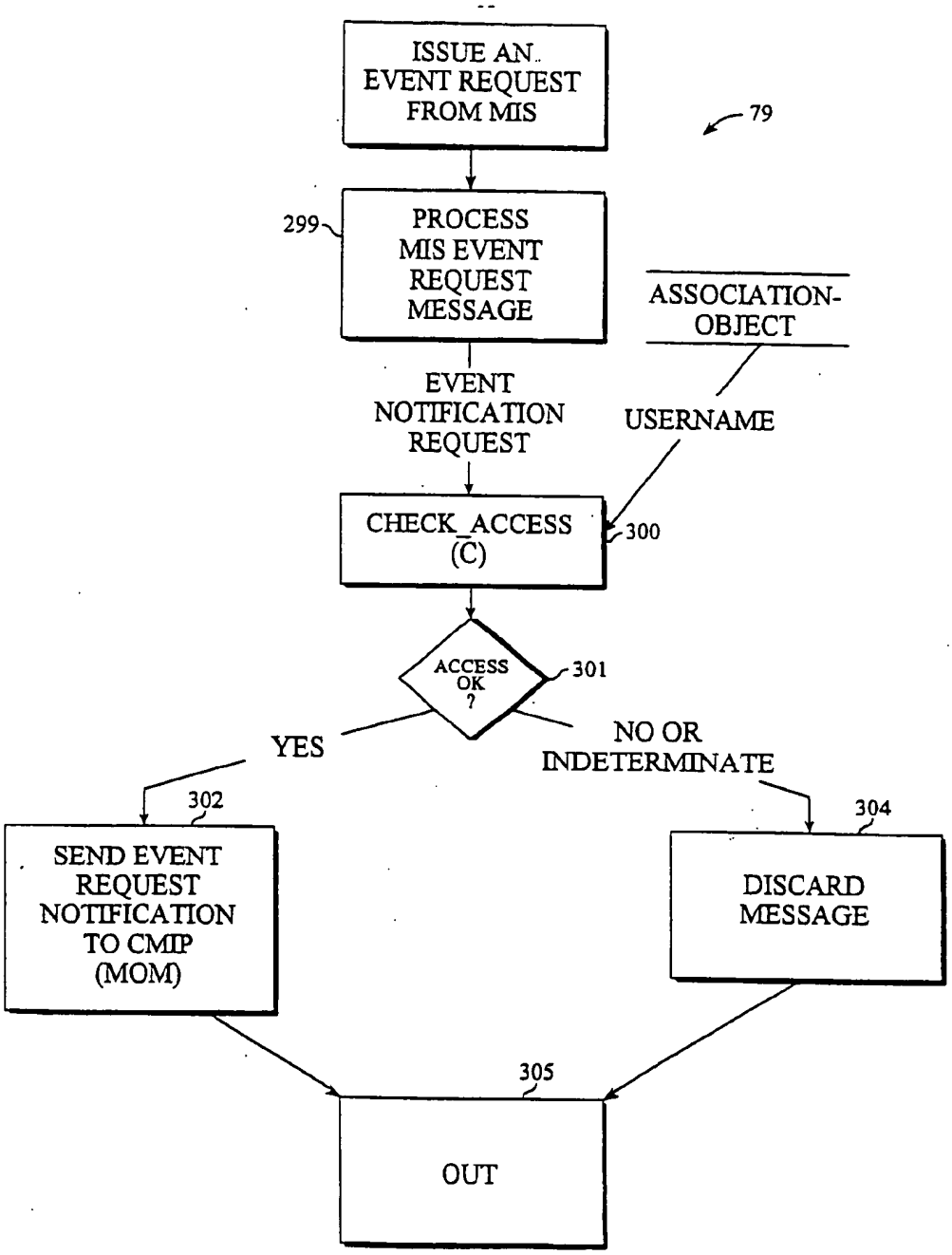

ISSUE AN EVENT REQUEST FROM MIS
79
299
PROCESS MIS EVENT REQUEST MESSAGE
ASSOCIATION-OBJECT
EVENT NOTIFICATION REQUEST
USERNAME
CHECK_ACCESS (C)
300
ACCESS OK ?
301
YES
NO OR INDETERMINATE
302
304
SEND EVENT REQUEST NOTIFICATION TO CMIP (MOM)
DISCARD MESSAGE
305
OUT

Fig. 10

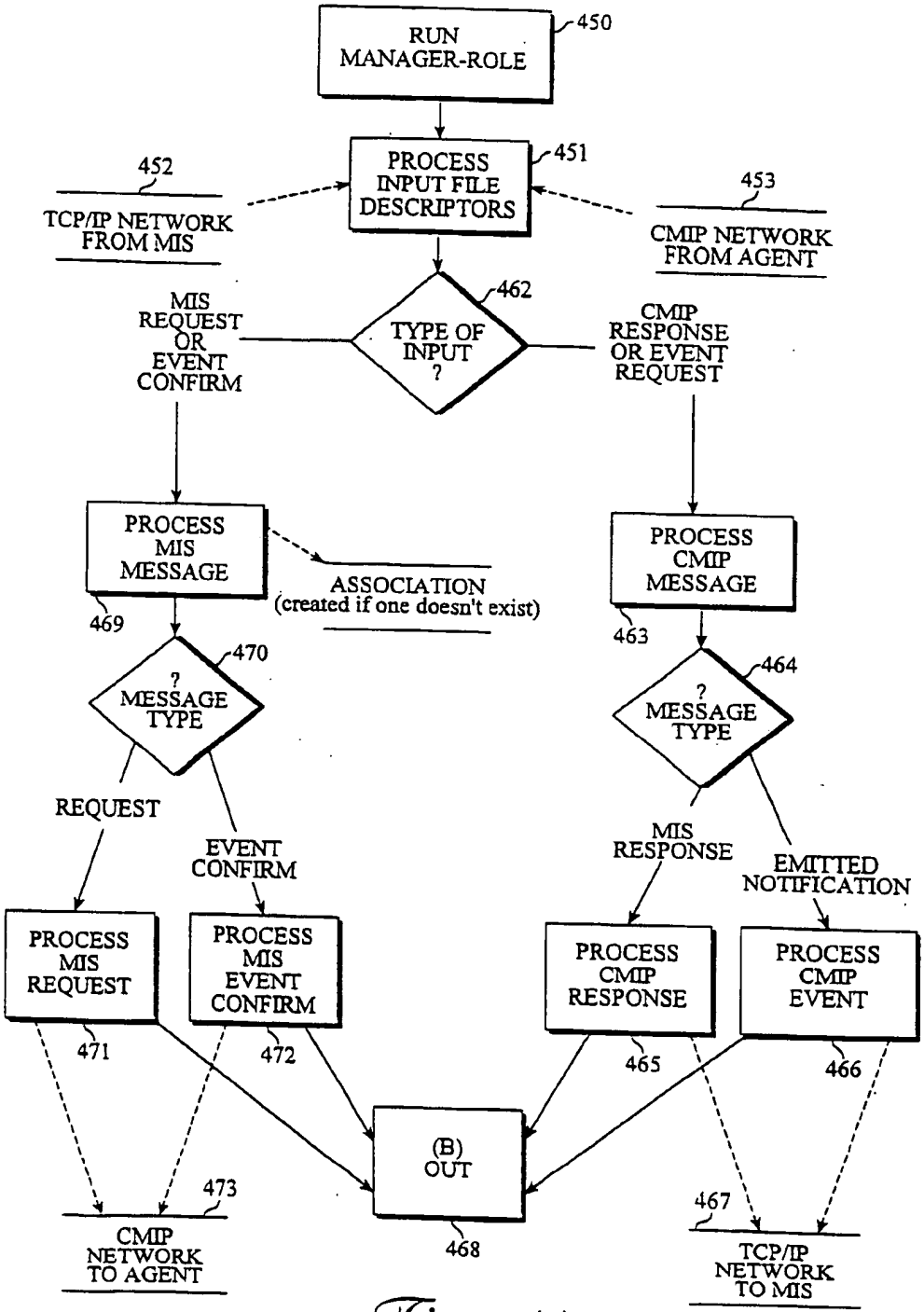

RUN MANAGER-ROLE
450
PROCESS INPUT FILE DESCRIPTORS
451
452
TCP/IP NETWORK FROM MIS
453
CMIP NETWORK FROM AGENT
462
TYPE OF INPUT ?
MIS REQUEST OR EVENT CONFIRM
CMIP RESPONSE OR EVENT REQUEST
PROCESS MIS MESSAGE
469
ASSOCIATION (created if one doesn't exist)
PROCESS CMIP MESSAGE
463
470
? MESSAGE TYPE
464
? MESSAGE TYPE
REQUEST
EVENT CONFIRM
MIS RESPONSE
EMITTED NOTIFICATION
PROCESS MIS REQUEST
PROCESS MIS EVENT CONFIRM
PROCESS CMIP RESPONSE
PROCESS CMIP EVENT
471
472
465
466
(B) OUT
468
473
CMIP NETWORK TO AGENT
467
TCP/IP NETWORK TO MIS

Fig. 11

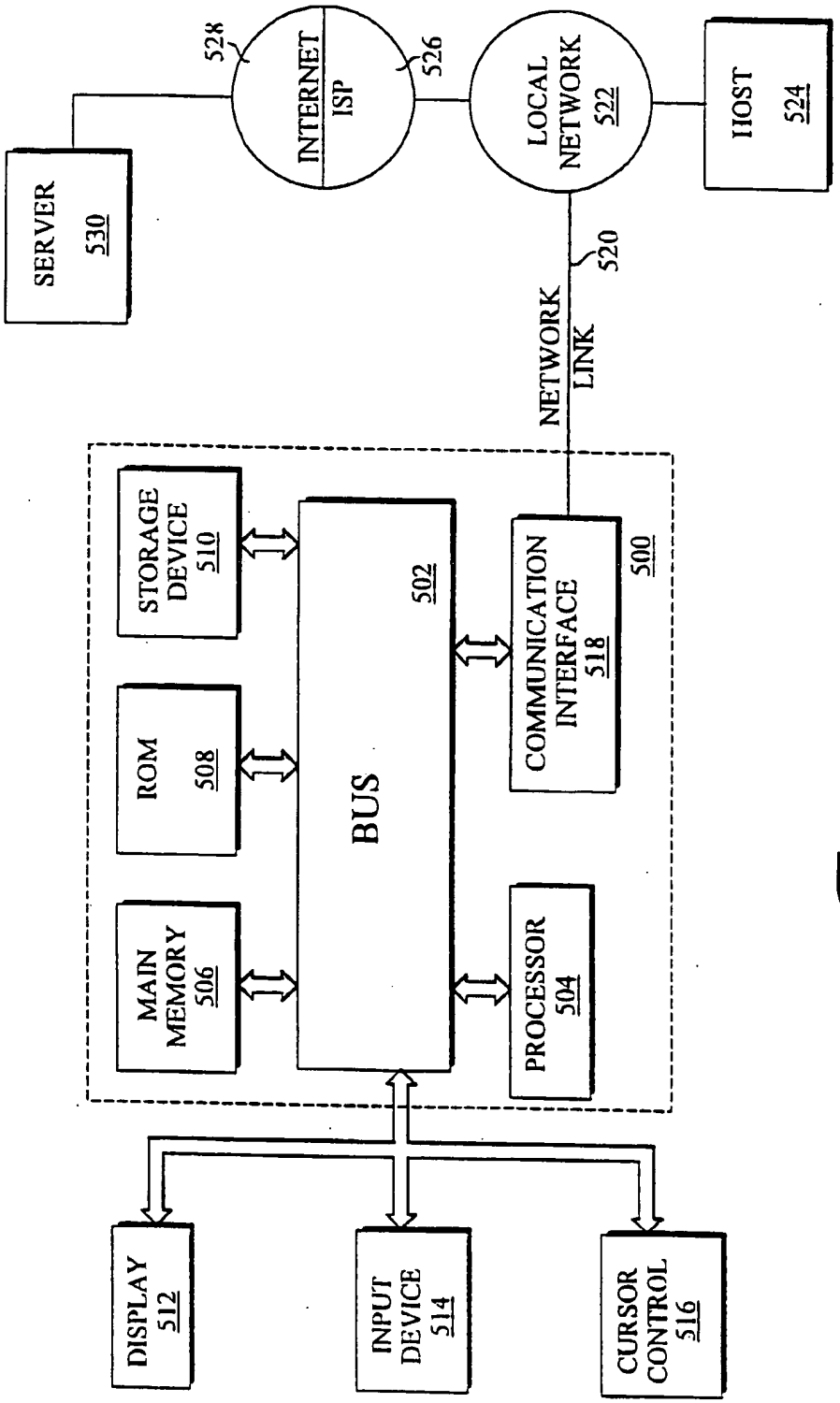

SERVER
530
INTERNET
ISP
528
526
LOCAL
NETWORK
522
HOST
524
NETWORK
LINK
520
STORAGE
DEVICE
510
ROM
508
MAIN
MEMORY
506
BUS
502
COMMUNICATION
INTERFACE
518
500
PROCESSOR
504
DISPLAY
512
INPUT
DEVICE
514
CURSOR
CONTROL
516

Fig. 12

APPARATUS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR NETWORK MANAGEMENT OPERATIONS RELATING TO NETWORK MANAGEMENT PROTOCOL ADAPTER SECURITY SOFTWARE (MPASS) FOR MESSAGING WITH USER NAME ACCESS IDENTIFICATION

CROSS REFERENCE TO RELATED PATENT APPLICATIONS

This patent application is related to other patent applications, filed herewith on the same day and entitled "Apparatus, Methods and Computer Program Products For Network Management Operations Relating To Network Management Protocol Security Software (MPASS) For Single and Multiple Users", Ser. No. 09/330,902, Secure User Association and Set-Up Using Network Management Protocol Security Software (MPASS)", Ser. No. 09/330,932.

"Independent Log Containment Hierarchy", Ser. No. 09/330,514, "Domain Access Control For Logging Systems", Ser. No. 09/332,270, and "Distinguished Name Scoping System For Event Filtering", Ser. No. 09/330,790. These related patent applications are hereby expressly referenced and incorporated herein in their entirety.

COPYRIGHTS IN PATENT MATERIALS

Portions of this patent document contain material subject to copyright restriction. The copyright owner has no objection to facsimile reproduction of the patent document after grant, as it appears in the U.S. Patent and Trademark Offices files or records, but otherwise reserves all rights relating thereto.

TECHNICAL FIELD

The field of this application relates to apparatus, methods, and computer program products relating to network management operations and particularly to apparatus, methods, and computer program products for network management protocol adapter security software.

BACKGROUND OF THE INVENTION

Currently, remote network management entities can gain access to local network management entity management information completely. This is particularly desired by enterprises which are leasing network bandwidth from carriers which have used large-scale network management frameworks to consolidate network management functions for all of the pieces of a leased network into a single platform. An enterprise wants visibility into the part of the network which it has leased. Carriers offer their customers visibility into the network management framework so that customers can see what is happening to the portion of the network they have leased. This is done by a network management system owned by the customer. This network management system communicates with the network management system owned by the carrier using a protocol such as Common Management Information Protocol (CMIP).

In particular, the customer asks for the status of managed objects owned by the customer. Both local and remote users of the network management system interact with the network management information as a set of objects. When a carrier's network management system receives commands from multiple customers A and B, each requesting visibility into a corresponding portion of the network, the carrier's network management system needs to ensure that customer

A does not see customer B data and vice-versa. It is desirable to restrict such remote access to local network management information. A local user of a management system has its use of the management system and its features and objects restricted by native security features built into the network manager and the computer system itself. However, a remote network management application entity may not be specifically identifiable as a user-id on a host computer system. Accordingly, the local network manager may not be able to exploit the security features of the host computer system to restrict access.

It is further desirable that the view presented to a remote network manager of the local management information tree (MIT) be pruned to include only selected information items. It is technically difficult to implement such restrictions, limitations, and prohibitions. In particular, standard network management protocols, such as the Common Management Information Protocol (CMIP), set forth in International Telecommunication Union (ITU) Standard x.711), provide hooks to install proprietary authentication and authorization, but fail to include standardized authentication and authorization mechanisms.

SUMMARY OF THE INVENTION

A computer implemented method and a computer program product according to the present invention, includes a first computer readable code construct configured to handle request messages. This comprises receiving a request message and having an associated user name which is associated with a remote user on a network. Further according to the present invention, making an access determination to determine whether the forwarding of the request message is authorized, and finally when forwarding of the request message is authorized, the message to a target system is forwarded.

According to one embodiment of the present invention, a computer implemented method and a computer program product include a first computer readable code construct configured to handle request messages. This comprises receiving a request message and having an associated user name which is associated with a remote user on a network. Further, making an access determination to determine whether the forwarding of the request message is authorized, and finally when forwarding of the request message is authorized, the message to a target system is forwarded. The MPASS feature provides an open-system approach of agent role authorization and authentication that can be used in interactions with any other management system. According to the present invention, the management protocol adapter security software (MPASS) feature enables a network manager, acting in an agent role, to restrict access to its management information over CMIP communications, with respect to remote network management entities. MPASS allows a network manager to identify remote CMIP network management entities as specific users and to restrict their access to its management information. In particular, according to one embodiment of the present invention, an authentication/authorization mechanism is automatically enforced by a Solstice Enterprise Manager (SEM) framework when the local network management entity receives a remote request, to ensure that only appropriate, limited visibility is provided to peers and superior managers requesting local network management information.

Further, according to the present invention, when multiple users have access to a shared management system, the carrier's network management framework authenticates and

assigns a user name to each MOM and peer manager who connects and provides access control over particular requests, so that each customer sees only the appropriate limited portion of the data stored in the network management framework which the customer is entitled to access. According to the present invention, access to features and objects of the network management system is restricted to particular remote users, who are either assigned a user-id, mapped from their network address and application-entity title, or is optionally assigned a fallback or default user-id.

According to one embodiment of the present invention, a remote user-id is assigned to the remote network management system, to enable the local system to identify its authorization scope.

According to another embodiment of the present invention, a remote user-id is assigned to the remote network management system based upon the remote entity network address and application title, to enable the local system to identify its authorization scope. The MPASS system, according to the present invention, restricts access to local management information by remote network management entities communicating over ITU x.711 CMIP using ITU x.227 ACSE (Association Control Service Element) connections, referred to as associations. The local management information is made available to a remote management entity in the entity's native network management protocol using management protocol adapters (MPAs) specific to the local manager. Each of the remote applications of the remote managers is identified by an MPA as a remote user with a specific network address and application-entity-title (AE-title), as described in ITU Standard x.650. An AE-title is a presentation layer address, added as a supplement to allow this layer to distinguish different applications that are active at the OSI layer 7, the application layer.

With an MPASS single user feature configured according to the present invention, a specified MPA is assigned a user-id. The MPA and assigned user-id are reserved for a single user, and the MPA restricts access to the management information allowed by that user's access permissions. With a multi-user feature of MPASS according to the present invention, a specified MPA is assigned zero or more user-ids mapped to the MPA network address and AE-title. With these user-ids, access is restricted by the local manager to only allow associations of specified users. Accordingly, the MPA only presents to a remote user the management information allowed by that remote user's access permissions.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system including a network operation center (NOC) superior manager, that is, a manager of managers (MOM);

FIG. **2** is a flowchart of an MPASS method according to the present invention;

FIG. **3** is a flow chart of an MPASS access control initialization method according to one embodiment of the present invention;

FIG. **4** is a flow chart of a method of run agent operation according to one embodiment of the present invention;

FIG. **5** is a flow chart of a check access method according to one embodiment of the present invention;

FIGS. **6**A and **6**B are a flow chart of a new association method according to one embodiment of the present invention;

FIG. **7** is a flow chart according to the present invention of a method of processing CMIP event confirm response messages;

FIG. **8** is a flow chart according to the present invention of a method of processing CMIP request messages;

FIG. **9** is a flow chart according to the present invention of a method of processing MIS response messages;

FIG. **10** is a flow chart according to the present invention of a method of processing CMIP event request messages;

FIG. **11** is a flow chart of a method of run manager operation according to one embodiment of the present invention; and

FIG. **12** is a block diagram of a computer system which may be used to implement the present invention.

DETAILED DESCRIPTION OF A PREFERRED MODE

Referring now to FIG. **1**, there is shown a block diagram of a computer system **1** including one or more network operation center (NOC) managers of managers (MOM-**1**, MOM-**2**, . . . , MOM-N) **2**. The computer system **1** further includes a first network system **3** connected to the one or more MOMs **2**, an enterprise manager (EM) **4**, a second network system **5**, and one or more agents **6** such as agent A, . . . , agent M for example, according to the present invention. According to one embodiment of the present invention, the EM **4** includes a CMIP MPA agent **7**, which optionally is assigned a fallback user id, an EM management information system (MIS) intermediate, peer, or subordinate manager (EMIM) **8** acting in a subordinate management role, and a CMIP MPA manager **9**. The EMIM **8**, in turn, includes a management information tree (MIT) **10** which has mapped into it as objects a multi-user access map (UAM) containing an access table of user-ids. A single user fallback user-id is directly mapped into the CMIP MPA from its environment variables or the command line.

The UAM is a branch of the MIT that stores user-ids and the network addresses of peer or superior managers. Each remote entity may have one entry in the UAM. A presentation layer address and an application-entity title form a key that is used by the CMIP MPA in an agent role to retrieve a specific user name from the UAM.

Referring now to FIG. **2**, there is shown a top level flowchart of an MPASS method **19** according to the present invention. The MPASS method **19** begins **20** with session initialization of a connection with the CMIP stack (i.e., binding to the CMIP stack), followed by establishment of a connection to the MIS, and finally a session with the security subsystem, an access control engine (ACE). Once the session is initialized, the CMIP MPA **21** runs in first and second predetermined roles, including operation in an agent role and operation in a manager role, as discussed in greater detail below. In particular, the CMIP MPA **21** runs the agent role and the manager role logic in the loop of a finite state machine. Three primary error conditions that cause the CMIP MPA to exit the state machine and to terminate execution are: the detection of a non-recoverable error returned from the CMIP stack, the occurrence of internal error in the CMIP MPA **21**, and the entry of the CMIP MPA **21** into a retry timeout loop in which it stays until successful reconnection to the MIS is accomplished. After the CMIP MPA **21** has been initialized with respect to an MIS connection, according to an initialization test **22**, the MPASS agent role access control system is initialized **23** to initiate an ACE security session with the MIS. Once the MPASS access control system has been initialized **24**, the EM performs in an agent role which is run **25**, as discussed in detail herein.

Alternatively, the EM operates in a manager role which is run **26** according to a predetermined sequence and architec-

ture. By callback, a check is armed continuously **27** to determine whether the MIS has been disconnected **27**. If the MIS is disconnected, the agent role and the manager role of the EM are rerun **25**. A stack check is armed continuously **28** to determine if a stack failure condition has occurred. If no stack failure or kill condition has been encountered in either the agent role or the manager role, the agent role of the EM experiences no changes If there has been such a failure or stack kill of the MIS, the EM exits and quits operation **29**. In summary, the initialization of the CMIP MPA requires an MIS connection **30** to be completed.

Referring now to FIG. **3**, there is shown an MPASS access control initialization method **39** for ensuring security to local management information, according to one embodiment of the present invention. The MPASS access control method **39** includes initializing an MPASS access control **23** subsystem, followed by initialization **41** of an access control engine (ACE) of the access control subsystem. Then, registration **42** is accomplished for predetermined ACE access control change events. Accordingly, callback functions are created **47** pursuant to registration of ACE access control change events. Then, a user access map (UAM) is obtained **43** from an MIT according to the present invention. This user access map is obtained from a UAM source **48** in the MIT, according to one embodiment of the present invention. Next, the UAM is cached **44** for use in MPASS. In particular, cacheing is implemented by local storage of the UAM **49**. Thereafter, fallback user information is cached **45** from a command-line to a fallback-user memory location **50**. Thereafter, an exit is taken **46** from the MPASS initialization access control routine **39** according to an embodiment of the present invention.

Referring now to FIG. **4**, there is shown a method of run agent operation **59** for the EM, according to one embodiment of the present invention. The agent role of the EM has a run status **60** according to the present invention which includes processing **61** input file descriptors which are predetermined. In particular, an evaluation is made **62** as to the type of input received, i.e., either an input from the MIS or an input from the CMIP stack. The evaluation further is based upon MIS and CMIP file descriptors from a common management information service element (CMISE), or from an Association Control Service Element (ACSE) message or from a callback.

CMISE Message types according to one embodiment of the present invention include M-Event-Report, M-Get, M-Cancel-Get, M-Set, M-Action, M-Create, and M-Delete types of messages. These seven types of CMISE services provide many of the commands needed to transmit and process management information within the system. An M-Event-Report reports an event concerning a managed object to a CMISE service user and may be confirmed (or acknowledged) or unconfirmed. An M-Get message requests retrieval of management information from a peer CMISE service user and requires confirmation. An M-Cancel-Get message requests that a peer CMISE service user cancel a previously requested and currently outstanding request made using an M-Get message and requires confirmation. An M-Set message requests modification of management information by a peer CMISE service user and may be confirmed or unconfirmed. An M-Action message requests that a peer CMISE service user perform a specified action and may be confirmed or unconfirmed. An M-Create message requests that a peer CMISE service user create an instance of a managed object and requires confirmation. An M-Delete message requests that a peer CMISE service user deletes specified instances of managed objects and requires confirmation.

ACSE messages are exchanged for creating or leaving class associations (connections). The agent role CMIP MPA receives ACSE indications (requests) for initiation of a link or association, and the ACSE issues either an ACSE response (success), and ACSE abort (for abrupt termination) or an ACSE release (for an orderly termination).

An M-Event-Report message conveys management information applicable to a notification. The other six types of services convey information applicable to systems management and operations. The M-Get, M-Set, M-Action and M-Delete messages can specify operation on single or multiple objects. When multiple objects are specified, if the request is successful, one response is returned for each object. Linkage between multiple responses is provided by a linked identifier parameter, which appears in each response and confirm message.

In one instance of operation of the EM, a CMIP message is received and processed **63** upon reception from a CMIP network **80**, based upon a new association, ACSE request indication, request or an event confirmation type of input. In at least one of such cases of receipt of a CMIP message, a determination of message type is made **64**. Then, confirmation of receipt of the CMIP event is sent **65** to the MIS. Finally, the run agent role of the EM is completed **71**.

According to another instance of operation of the run agent role of the CMIP MPA **7**, a TCP/IP MIS message is received from an associated TCP/IP network **79** and the particular MIS message received is processed **76**, according to a predetermined scheme, and a CMISE response or a CMISE event notification request. In particular, a determination is made as to message type **77**, such as response, request, or notification. A response message is sent **78** to the CMIP stack without an access check, because the access check was already performed on the original request. An access check is conducted **67** with the MIS security mechanism, the ACE, in particular to authenticate access requests and notifications. The access check is either successful, indeterminate, or a failure. Where authorization of access is indeterminate, an event notification is discarded, and the operation is considered to be completed **71**. When a CMIP request is received from a remote manager such as MOM-2 for local management information, an access check is performed with the MIS security system (ACE. The access check is successful, is indeterminate, or fails. For a request, if successful, the request is sent to the MIS. If the request access check is indeterminate, the request is sent to the MIS and receives additional security subsystem checks, before being processed. If the request access check is a failure, the request is discarded.

Referring now to FIG. **5**, there is shown a check access method **89** according to one embodiment of the present invention. In particular at the beginning **67** of the check access method **89**, a determination is made **90** of whether access control is in an on state or off state. If access control is off, no access check is performed, and the message is forwarded to its destination. If access is on, if the message type is an M-Cancel-Get message, the message is forwarded to the MIS without an access check. If the message type is one of an M-Event request type, or an M-Set request type, or an M-Action request type, or a M-Get request type, or an M-Delete type, or an M-Create type, the user name which was originally retrieved from the UAM or from the fallback user, and which is now stored in the association object, is encoded, added to the message and an ACE access check is performed. The access check response, one of success, indeterminate, and failure is returned.

Referring now to FIGS. **6A** and **6B**, there is shown a new association method **110** according to one embodiment of the

present invention. The new association begins **66** with processing of an association request (AARQ) **112** from a remote address **126** representing a remote management entity, subject to restrictions arising from resource limits **127** and certain overload limits **128**. The resource and overload limit information is determined from current state variables within the CMIP MPA. Thereafter, a determination is made as to whether to accept a new association **113** with a remote manager, based upon the current resource or overload limits or conditions. If new associations are acceptable, a determination is made whether processing is below overload thresholds **114**. If the answer is "yes" the processing is below overload conditions and a new association is created **116**. If the processing would exceed overload conditions, the attempted association is aborted **115**. Thus, operation is completed **125**, according to one path.

To create a new association **116** if the overload threshold has not been exceeded, a username is obtained **117** from the UAM **11** using the remote presentation address and AE-title of MOM as a key. Portions of the presentation address or the AE-title may hence be used as a pattern match to locate a specific user-id. If the username is found **118** in the UAM **11**, the particular UAM username which is found is assigned to the association **119**. Then, an association accept response message (AARE) is sent **126**. Otherwise, if the user is not found to be present in the UAM **11**, the fallback user is established **121**, and a determination is made whether the fallback user has been found **122**. If the answer is "yes", the fallback user has been found, that fallback user name which has been determined is assigned **123** to the association which has been accepted. Then, an accept response message (AARE) is sent **126**. Otherwise, if no fallback user has been found, a null user is assigned as a default, according to one embodiment of the present invention. Then, an AARE is sent **126**, followed by completion of new association operation **125**. The system allows acceptance of the association in this case, because it is possible that an appropriate user-id might be assigned in the UAM or fallback user object at a later time.

Referring now to FIG. **7**, there is shown a flow chart according to the present invention of a method **65** of processing CMIP event confirm response messages. In particular, according to the method **65**, a CMIP event confirm response is processed by receipt of a CMIP event confimation response **269** and then an event confirmation is sent to the MIS **270**, followed by an exit from CMIP event confirm response processing.

Referring now to FIG. **8**, there is shown a flow chart according to the present invention of a method **67** of processing CMIP request messages. According to the method **67**, a CMIP request message is processed **279** by receipt of a request indication followed by implementation of check access processing **280** based upon receipt of a username from an association object. Then a determination is made as to whether access rights are granted or not to enable handling of the CMIP request. If access rights are granted, the request is sent **282** to the MIS. If access rights are not granted, the message is discarded **284**. If the result of the access check is indeterminate, a request is sent **283** to the MIS security system for evaluation, followed by an exit **285** from CMIP request message.

Referring now to FIG. **9**, there is shown a flow chart according to the present invention of a method **78** of processing MIS response messages. In particular, according to the method **78**, an MIS response message is processed after receipt of the message, followed by an exit from CMIP event confirm response processing.

Referring now to FIG. **10**, there is shown a flow chart according to the present invention of a method of processing CMIP event request messages. According to the method **79**, a CMIP request message is processed **299** by receipt of an event notification request, followed by implementation of check access processing **300** based upon receipt of a username from an association object. Then a determination is made **301** whether access rights are granted or not to enable handling of the CMIP event request. If access rights are granted, the event notification is sent **302** to the CMIP. If access rights are not granted or are indeterminate, the message is discarded **304**.

Referring now to FIG. **11**, there is shown a flow chart of a method **450** of manager role operation according to one embodiment of the present invention. The management role of the EM has a run status, according to the present invention, which includes processing **451** input file descriptors which are received **452** over the TCP/IP network from the MIS or over the CMIP network **453** from an agent. In particular, an evaluation is made **462** as to the type of input received, i.e., either an input from the MIS or an input from the CMIP stack. The evaluation further is based upon MIS and CMIP file descriptors from a CMISE message or from a callback. Message types according to one embodiment of the present invention include M-Event-Report, M-Cancel-Get, M-Get, M-Set, M-Action, M-Create, and M-Delete types of messages. In one instance of operation of the EM, a CMIP message is received and processed **463** upon reception from a CMIP network **453**. In at least one case of receipt of a CMIP message, a determination of message type is made **464**. Then, confirmation of receipt of the CMIP event is sent **465** to the MIS Finally, the run management role of the EM is completed **468**.

According to another instance of operation of the run management role of the CMIP MPA **7**, a TCP/IP MIS message is received from an MIS associated TCP/IP network **452**, the particular MIS message received is processed, according to a predetermined scheme, and a CMISE request or a CMISE event notification confirmation response is processed. In particular, a determination is made as to message type **469**, e.g., request or event confirmation. A response message is sent to the CMIP stack without an access check, because the access check was already performed on the original request. An access check is conducted with the MIS security mechanism (ACE) to perform access checks for requests and notifications. The access check either proves to be successful, is indeterminate, or is a failure. In the event of access authorization being indeterminate, an event notification is discarded and the operation is considered to be completed. When a CMIP request is received from a remote manager such as MOM-2 for local management information, an access check is performed with the MIS security system (ACE. The access check is one of success, indeterminacy, or failure. If a request access check is successful, the request is sent to the MIS. If the request access check is indeterminate, the request is sent to the MIS and receives additional security subsystem checks before being processed. If the request is a failure, the request is discarded.

FIG. **12** shows a block diagram of a general computer system **500** which may be used to implement various components of the present invention. Computer system **500** includes a bus **502** or other communication mechanism for communicating information, and a processor **504** coupled with bus **502** for processing information. Computer system **500** also includes a main memory **506**, such as a random access memory (RAM) or other dynamic storage device,

coupled to bus **502** for storing information and instructions to be executed by processor **504**. Main memory **506** also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor **504**. Computer system **500** further includes a read only memory (ROM) **505** or other static storage device coupled to bus **502** for storing static information and instructions for processor **504**. A storage device **510**, such as a magnetic disk or optical disk, is provided and coupled to bus **502** for storing information and instructions. Computer system **500** may be coupled via bus **502** to a display **512**, such as a cathode ray tube (CRT), for displaying information to a computer user. An input device **514**, including alphanumeric and other keys, is coupled to bus **502** for communicating information and command selections to processor **504**. Another type of user input device is cursor control **516**, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor **504** and for controlling cursor movement on display **512**. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify positions in a plane. According to an embodiment, the functionality of the present invention is provided by computer system **500** in response to processor **504** executing one or more sequences of one or more instructions contained in main memory **506**. Such instructions may be read into main memory **506** from another computer-readable medium, such as storage device **510**. Execution of the sequences of instructions contained in main memory **506** causes processor **504** to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software. The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor **504** for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device **510**. Volatile media includes dynamic memory, such as main memory **506**. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise bus **502**. Transmission media can also take the form of acoustic or electromagnetic waves, such as those generated during radio-wave, infra-red, and optical data communications. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punchcards, papertape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read. Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor **504** for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system **500** can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector can receive the data carried in the infra-red signal and appropriate circuitry can place the data on bus **502**. Bus **502** carries the data to main memory **506**, from which processor **504** retrieves and executes the instructions. The instructions received by main memory **506** may optionally be stored on storage device **510** either before or after execution by processor **104**. Computer system **500** also includes a communication interface **515** coupled to bus **502**. Communication interface **515** provides a two-way data communication coupling to a network link **520** that is connected to a local network **522**. For example, communication interface **515** may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface **515** may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface **515** sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information. Network link **520** typically provides data communication through one or more networks to other data devices. For example, network link **120** may provide a connection through local network **522** to a host computer **524** or to data equipment operated by an Internet Service Provider (ISP) **526**. ISP **526** in turn provides data communication services through the world wide packet data communication network now commonly referred to as the "Internet" **525**. Local network **522** and Internet **525** both use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link **520** and through communication interface **515**, which carry the digital data to and from computer system **500**, are exemplary forms of carrier waves transporting the information. Computer system **500** can send messages and receive data, including program code, through the network(s), network link **520** and communication interface **515**. In the Internet example, a server **530** might transmit a requested code for an application program through Internet **525**, ISP **526**, local network **522** and communication interface **515**. The received code may be executed by processor **504** as it is received, and/or stored in storage device **510**, or other non-volatile storage for later execution.

In summary, according to the present invention, a computer-implemented method for network management operates in a computer system including a local network manager and at least one remote network manager (e.g., a remote user). A method according to the present invention includes, without limitation, receiving a request for management information from a remote network manager, and restricting access to management information in response to a request made by a remote network manager. A method of the present invention includes implementing communications between local and remote network managers using CMIP and processing a request by a remote network manager for local network management information, with the local network manager restricting access to the local management information. According to one embodiment of the present invention, access is restricted using a management protocol adapter security software (MPASS) feature. The method begins with initiation of communications between a local network manager a remote network manager. The remote network manager requests local network management information. The MPASS features enables a local network manager to act in an agent role to restrict access to its management information over CMIP communications with respect to a remote network manager. In particular, MPASS allows a network manager to identify particular

remote CMIP network management entities as specific users and to restrict their access to its management information according to a predetermined scheme.

The method according to another embodiment of the present invention includes enforcing an authentication or authorization mechanism automatically with an SEM framework. In particular, when the local network manager receives a remote network manager request, limited visibility is provided for the particular remote manager to ensure that only appropriate information is provided to the remote network manager. A local network manager is used, according to the present invention, to authenticate each remote network manager that connects, through a look-up table in the UAM, if possible, or use of a fallback user-id or null user-id. This provides access control over particular requests for local management information. Accordingly, each remote network managers sees only an appropriate limited portion of the local management information which is stored in a local network MIT, which each remote network manager is entitled to access.

In particular, the method of the present invention includes restricting access to features and objects of a local network manager to particular remote network managers. In particular, a user identifier (user-id) is assigned to each said remote network manager. The remote user-id is assigned to a remote network manager arbitrarily, according to one embodiment. This enables the local network manager to identify the authorization scope of particular remote network managers.

Further, according to the present invention, a remote user-id is assigned to zero or more remote network managers based upon particular associated network addresses and application titles. This enables the local network manager to identify the authorization scope of particular remote network managers that request information. Further, according to one embodiment of the present invention, the MPASS feature restricts access to local management information by remote network managers that communicate over ITU x.711 CMIP. More particularly, the network managers use ITU x.227 ACSE connections, referred to as associations.

According to one embodiment of the present invention, local network management information is available to remote network managers in their native network management protocol. To accomplish this result, an MPA specific to the local network manager is employed. According to one embodiment of the present invention, identifying remote applications of remote network managers is accomplished with an MPA. A remote user is thus provided with a specific network address and an AE-title (as described in ITU Standard x.650). Further, the method according to the present invention uses an MPASS single-user feature in which a specified MPA is assigned a particular user-id. With this user-id, the MPA is reserved for a single user. Further, the MPA then restricts access to local network management information according to that particular user's access permissions. According to a multi-user feature of MPASS, assignment is made of a specified MPA with zero or more user-ids, which are mapped from associated network addresses and application-entity titles as keys.

Further according to the present invention, a computer program product is embodied in a computer usable medium having a computer readable code means embodied therein. The computer program product is used for managing remote network manager requests for local network manager information. The computer program product particularly comprises a first computer readable code construct (CRCC) configured to receive a request for management information from a remote network manager. The computer program product further comprises a second CRCC configured to restrict access to management information in response to a request made by a remote network manager.

What is claimed is:

1. A computer program product embodied in a computer usable medium having a computer readable code means embodied therein, the computer program product comprising:

a first computer readable code means configured to receive a message, having an associated user name, from a remote user on a network;

a second computer readable code means configured to make an access determination to determine whether a response to the message is authorized;

a third computer readable code means configured to deliver the message to a management information system, referred to as an MIS, when forwarding of a request message is authorized; and

a fourth computer readable code means configured to allow the MIS to analyze the message and to prepare and forwarding a response message to the remote user.

2. The computer program product according to claim 1, wherein at least one of said first, second, third and fourth code means is configured to discard said message when forwarding of the request message is not authorized.

3. The computer program product according to claim 1, wherein at least one of said first, second, third and fourth code means is configured to make said access determination by:

determining if an access control protocol is activated;

when the access control protocol is not activated, indicating that forwarding the request message is authorized;

when the access control protocol is activated, determining what is the type of said message

when the message type is an M-Cancel-Get request, indicating that forwarding of the request message is authorized; and

when the message type is an M-Event request, an M-Set request, an M-Action request, an M-Get request, an M-Create request or an M-Delete request, performing an access check on said user name, and determining if the access check is successful, is indeterminate, or is unsuccessful.

4. The computer program product according to claim 3, wherein at least one of said first, second, third and fourth code means is configured to authorize forwarding a request message when said access check on said user name is successful.

5. The computer program product according to claim 4, wherein at least one of said first, second, third and fourth code means is configured to discard said message when said access check is not successful.

6. The computer program product according to claim 5, wherein at least one of said first, second, third and fourth code means is configured to perform at least one additional security check on said user name when said access check is indeterminate.

7. The computer program product according to claim 6, wherein at least one of said first, second, third and fourth code means is configured to authorize a response to said message when said access check is indeterminate and said at least one additional security check is successful.

8. A method of handling event request notifications, comprising:

determining if a peer or superior management entity (i.e., a MOM) is authorized to receive an event request; and

forwarding the event request to the MOM.

9. The method according to claim 8 wherein the event request is received from the MIS.

10. The method according to claim 8 wherein the event request is received from an agent subordinate to said MIS.

11. A method of handling request messages, comprising:

receiving a request for a new association from a remote network;

creating a first new association in response to determining new associations are being accepted;

accessing a predetermined user access map in order to obtain a username corresponding to said request, wherein said map is accessed using a presentation address and application entity title corresponding to said request;

assigning a first username obtained from said map to said first new association in response to detecting said first username corresponding to said presentation address and application entity title is present in said map; and

assigning a fallback username to said first new association in response to detecting said first username is not present in said map and said fallback username is present in said map.

12. The method according to claim 11, further assigning a null user to said first new association, in response to detecting said first username is not present in said map and said fallback username is not present in said map.

13. The method according to claim 11, further comprising receiving an request message from a manager of managers, said request message corresponding to said first new association.

14. The method according to claim 13, further comprising:

performing an access check on said request message, wherein said access check is based upon a received user name corresponding to said first new association;

sending said request message to a target management information server in response to determining access rights for said request message are granted;

forwarding said request message to a security system of the management information server in response to determining said access rights are indeterminate; and

discarding said request message in response to determining said access rights are not granted.

15. The method according to claim 14, wherein said access check comprises:

forwarding said message request to said management information server if said message request is a first type of message; and

performing an ACE access check on said message request if said message request is a second type of message.

16. The method according to claim 15, wherein said first type of message is an M-Cancel-Get message type, and wherein said second type of message is selected from the group consisting of: M-Event request type, M-Set request type, M-Action request type, a M-Get request type, M-Delete type, and M-Create type.

17. A system for handling messages, comprising a computer that is configured to:

receive a request for a new association from a remote network;

create a first new association in response to determining new associations are being accepted;

access a predetermined user access map in order to obtain a username corresponding to said request, wherein said map is accessed using a presentation address and application entity title corresponding to said request;

assign a first username obtained from said map to said first new association in response to detecting said first username corresponding to said presentation address and application entity title is present in said map; and

assign a fallback username to said first new association in response to detecting said first username is not present in said map and said fallback username is present in said map.

18. The system according to claim 17, wherein said computer is further configured to assign a null user to said first new association, in response to detecting said first username is not present in said map and said fallback username is not present in said map.

19. The system according to claim 17, wherein said computer is further configured to receive n request message from a manager of managers, said request message corresponding to said first new association.

20. The system according to claim 19, wherein said computer is further configured to:

perform an access check on said request message, wherein said access check is based upon a received user name corresponding to said first new association;

send said request message to a target management information server in response to determining access rights for said request message are granted;

forward said request message to a security system of the management information server in response to determining said access rights are indeterminate; and

discard said request message in response to determining said access rights are not granted.

21. The system according to claim 20, wherein said access check comprises:

forwarding said message request to said management information server if said message request is a first type of message; and

performing an ACE access check on said message request if said message request is a second type of message.

22. The system according to claim 21, wherein said first type of message is an M-Cancel-Get message type, and wherein said second type of message is selected from the group consisting of: M-Event request type, M-Set request type, M-Action request type, a M-Get request type, M-Delete type, and M-Create type.

* * * * *

US006484260B1

(12) **United States Patent**
Scott et al.

(10) **Patent No.: US 6,484,260 B1**
(45) **Date of Patent: *Nov. 19, 2002**

(54) **PERSONAL IDENTIFICATION SYSTEM**

(75) Inventors: **John D. Scott**, Galson (AU); **Terence Patrick Curtis**, Kariong (AU)

(73) Assignee: **Identix, Inc.**, Los Gatos, CA (US)

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/066,643**

(22) Filed: **Apr. 24, 1998**

(51) **Int. Cl.**[7] **H04K 1/00**
(52) **U.S. Cl.** **713/186**; 713/182
(58) **Field of Search** 380/23, 24; 382/124, 382/125, 126, 127, 115, 116, 313; 356/71; 340/825.34; 713/202, 182, 183, 184, 185, 186

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,623,552 A * 4/1997 Lane 382/124
5,770,849 A * 6/1998 Novis et al. 235/492
5,872,834 A * 2/1999 Teitelbaum 379/93.03
6,038,666 A * 3/2000 Hsu et al. 713/186
6,040,783 A * 3/2000 Houvener et al. 340/825.31
6,084,968 A * 7/2000 Kennedy et al. 380/259

OTHER PUBLICATIONS

Schneier, Bruce. Applied Cryptography, Second Edition. Schneier. 1995. See pp. 52–65 and 185–187.*
TouchNet II, Database and Network Access Control, 1997.

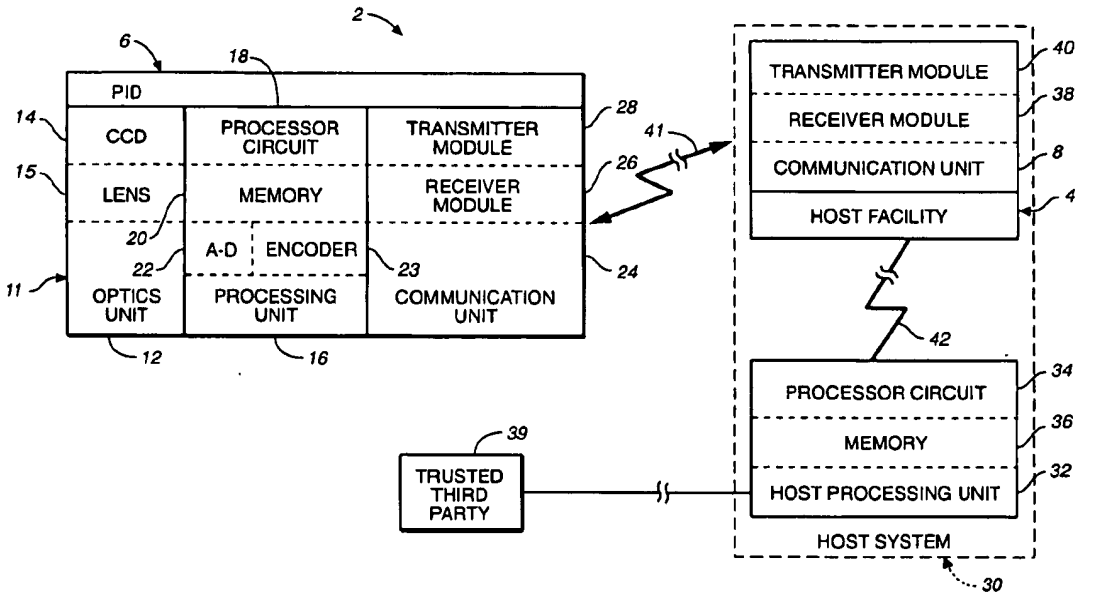
* cited by examiner

Primary Examiner—Gail Hayes
(74) *Attorney, Agent, or Firm*—Fish & Richardson P.C.

(57) **ABSTRACT**

A portable, hand-held personal identification device for providing secure access to a host facility includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait. A processing unit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is unique to the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal includes information indicative of the enrolled person or the device. A communication unit, including a transmitting circuit, is adapted to transmit the verification signal to a host system.

27 Claims, 12 Drawing Sheets



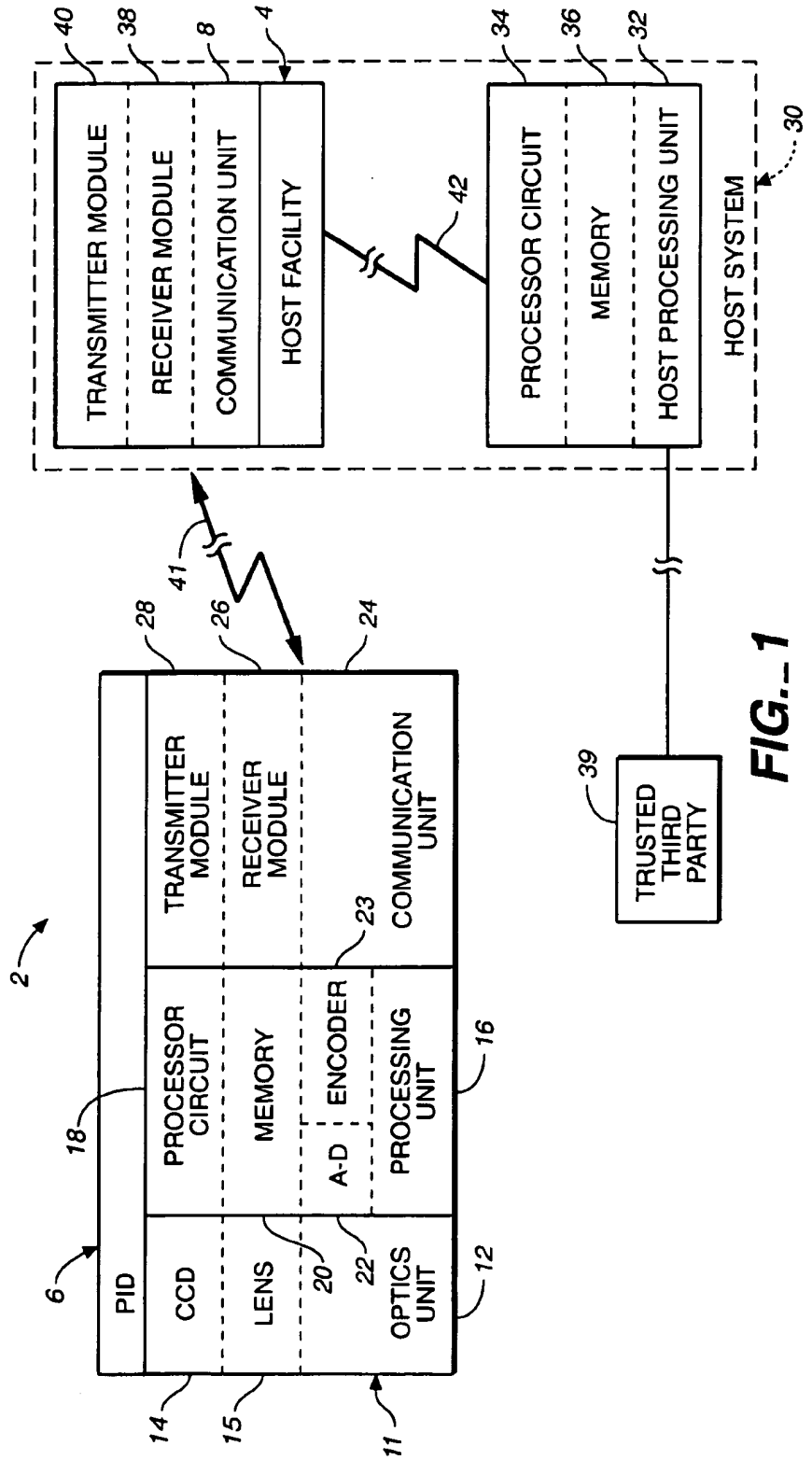

TRANSMITTER MODULE
RECEIVER MODULE
COMMUNICATION UNIT
HOST FACILITY
PROCESSOR CIRCUIT
MEMORY
HOST PROCESSING UNIT
HOST SYSTEM
TRUSTED THIRD PARTY
TRANSMITTER MODULE
RECEIVER MODULE
COMMUNICATION UNIT
PROCESSOR CIRCUIT
MEMORY
ENCODER
A-D
PROCESSING UNIT
PID
CCD
LENS
OPTICS UNIT
40
38
8
4
34
36
32
30
42
41
28
26
24
23
2
18
16
6
20
22
12
14
15
11
39

FIG._1

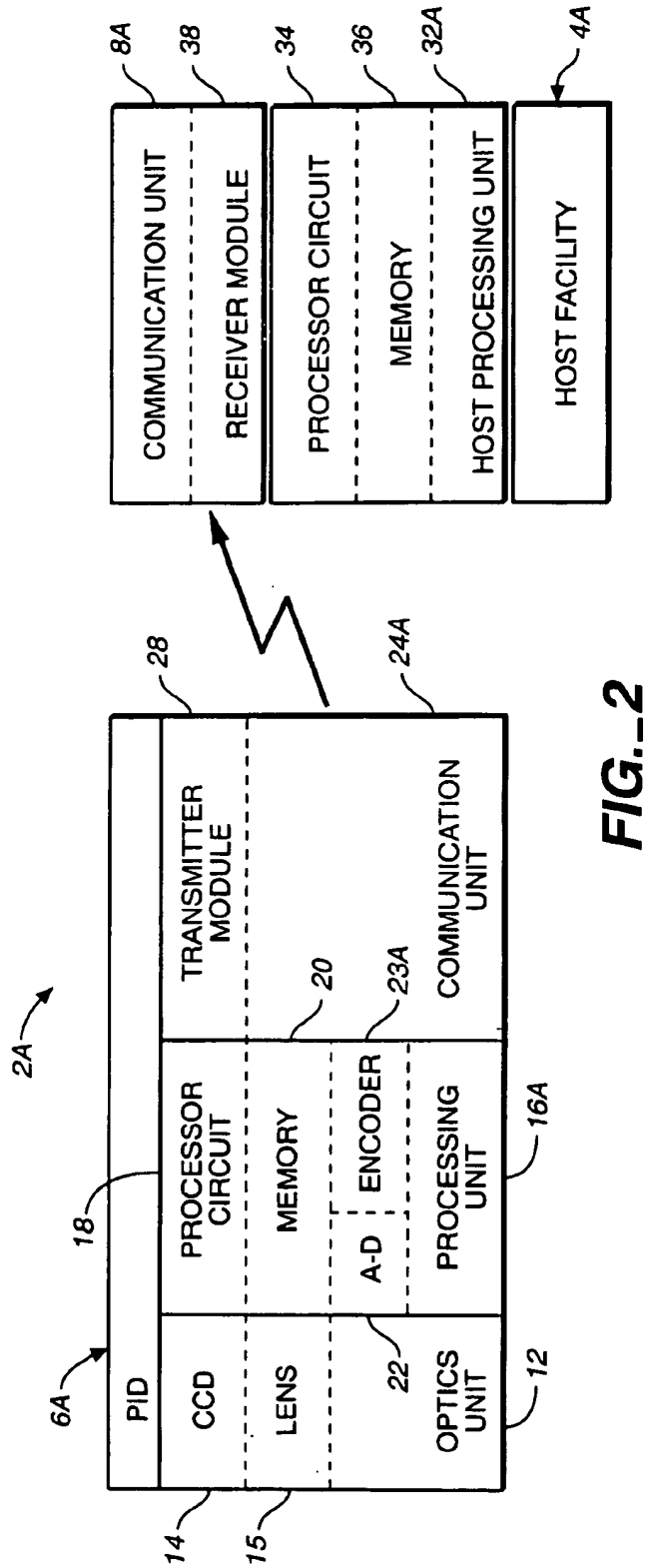

8A
38
34
36
32A
4A
COMMUNICATION UNIT
RECEIVER MODULE
PROCESSOR CIRCUIT
MEMORY
HOST PROCESSING UNIT
HOST FACILITY
28
24A
TRANSMITTER MODULE
COMMUNICATION UNIT
2A
20
23A
18
PROCESSOR CIRCUIT
MEMORY
A-D
ENCODER
PROCESSING UNIT
16A
6A
PID
CCD
LENS
22
OPTICS UNIT
12
14
15

FIG._2

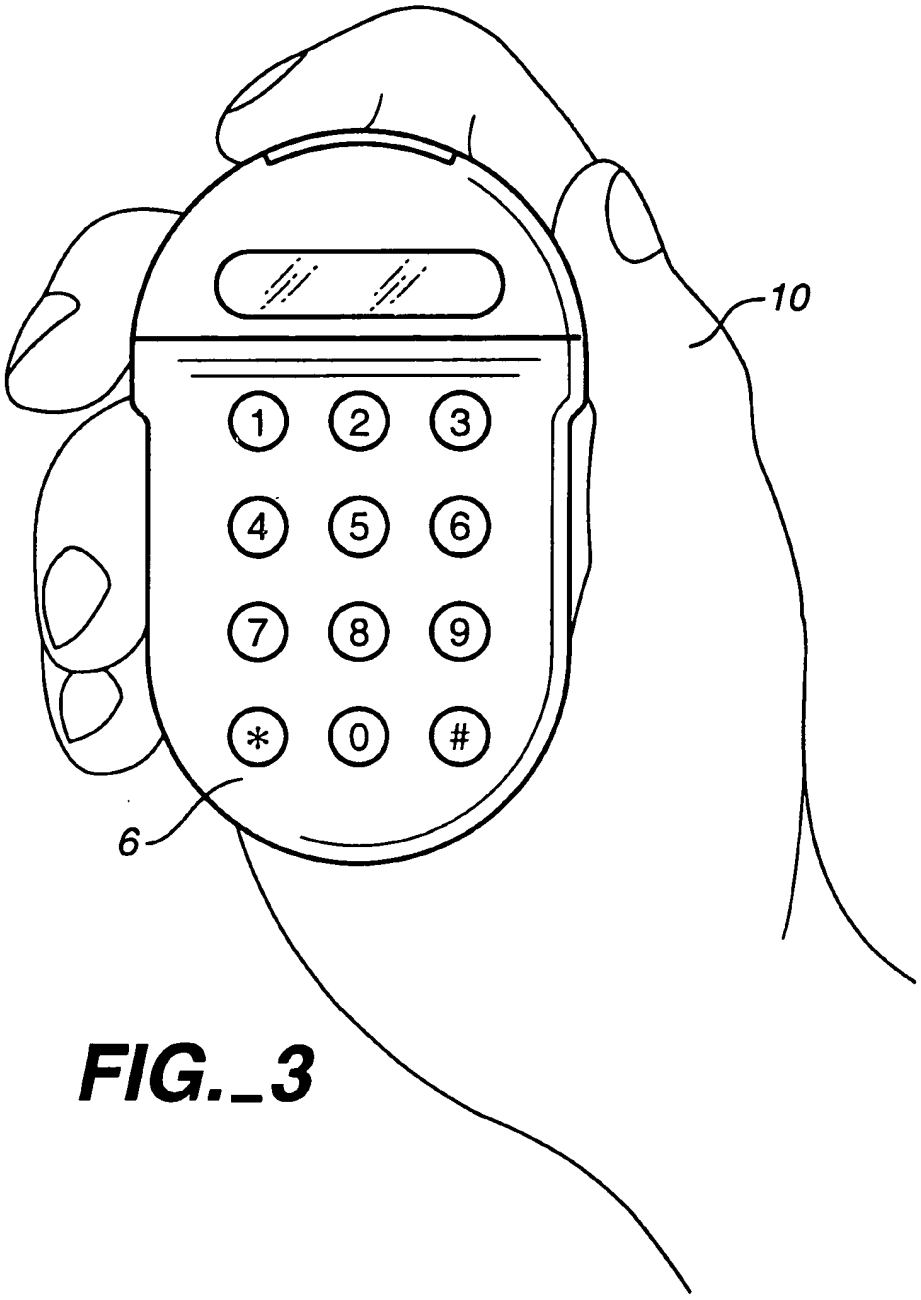


FIG._3

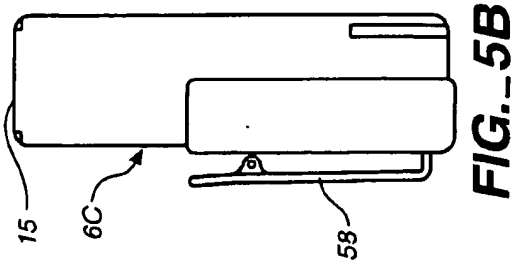


FIG._5B

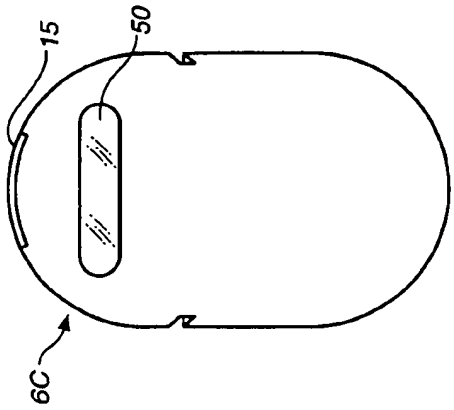


FIG._5A

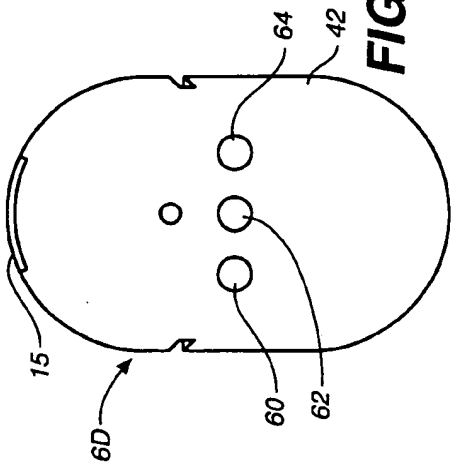


FIG._6

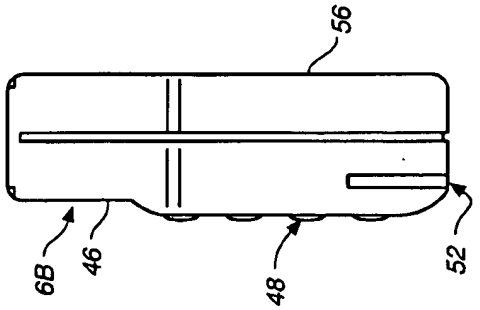


FIG._4B

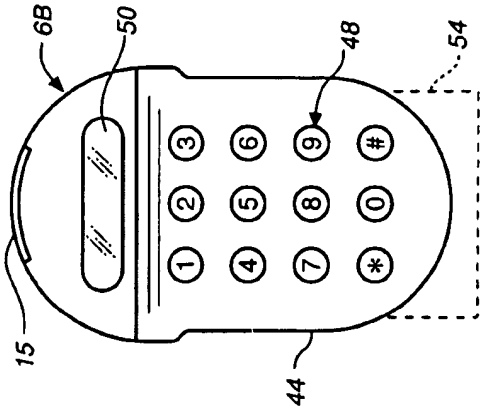


FIG._4A

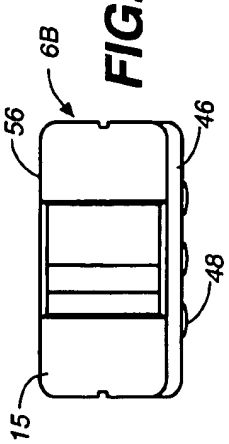


FIG._4C

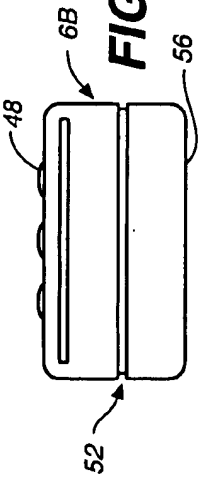


FIG._4D

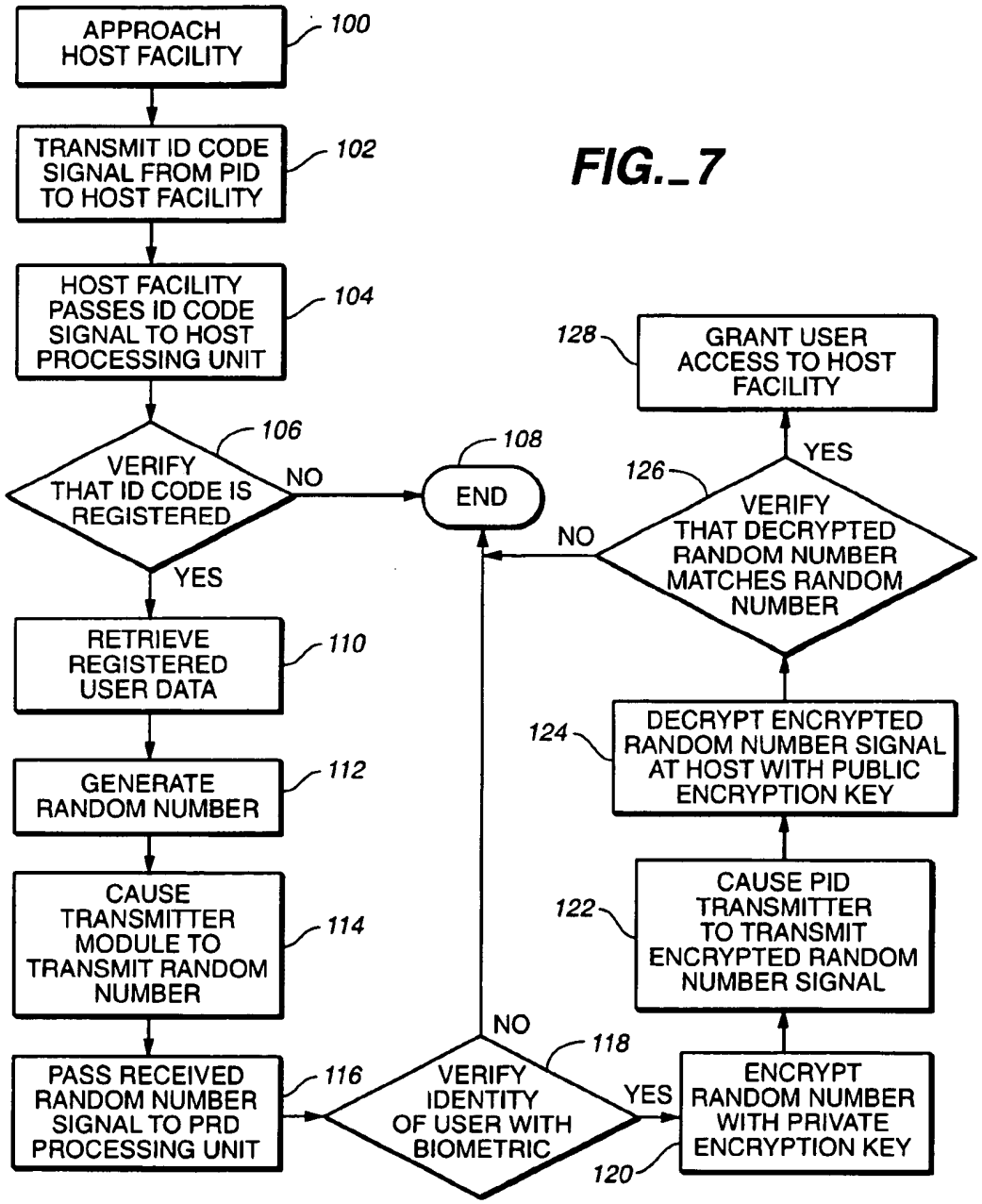

APPROACH HOST FACILITY
100
TRANSMIT ID CODE SIGNAL FROM PID TO HOST FACILITY
102
HOST FACILITY PASSES ID CODE SIGNAL TO HOST PROCESSING UNIT
104
VERIFY THAT ID CODE IS REGISTERED
106
NO
YES
END
108
RETRIEVE REGISTERED USER DATA
110
GENERATE RANDOM NUMBER
112
CAUSE TRANSMITTER MODULE TO TRANSMIT RANDOM NUMBER
114
PASS RECEIVED RANDOM NUMBER SIGNAL TO PRD PROCESSING UNIT
116
VERIFY IDENTITY OF USER WITH BIOMETRIC
118
NO
YES
ENCRYPT RANDOM NUMBER WITH PRIVATE ENCRYPTION KEY
120
CAUSE PID TRANSMITTER TO TRANSMIT ENCRYPTED RANDOM NUMBER SIGNAL
122
DECRYPT ENCRYPTED RANDOM NUMBER SIGNAL AT HOST WITH PUBLIC ENCRYPTION KEY
124
VERIFY THAT DECRYPTED RANDOM NUMBER MATCHES RANDOM NUMBER
126
NO
YES
GRANT USER ACCESS TO HOST FACILITY
128

FIG._7

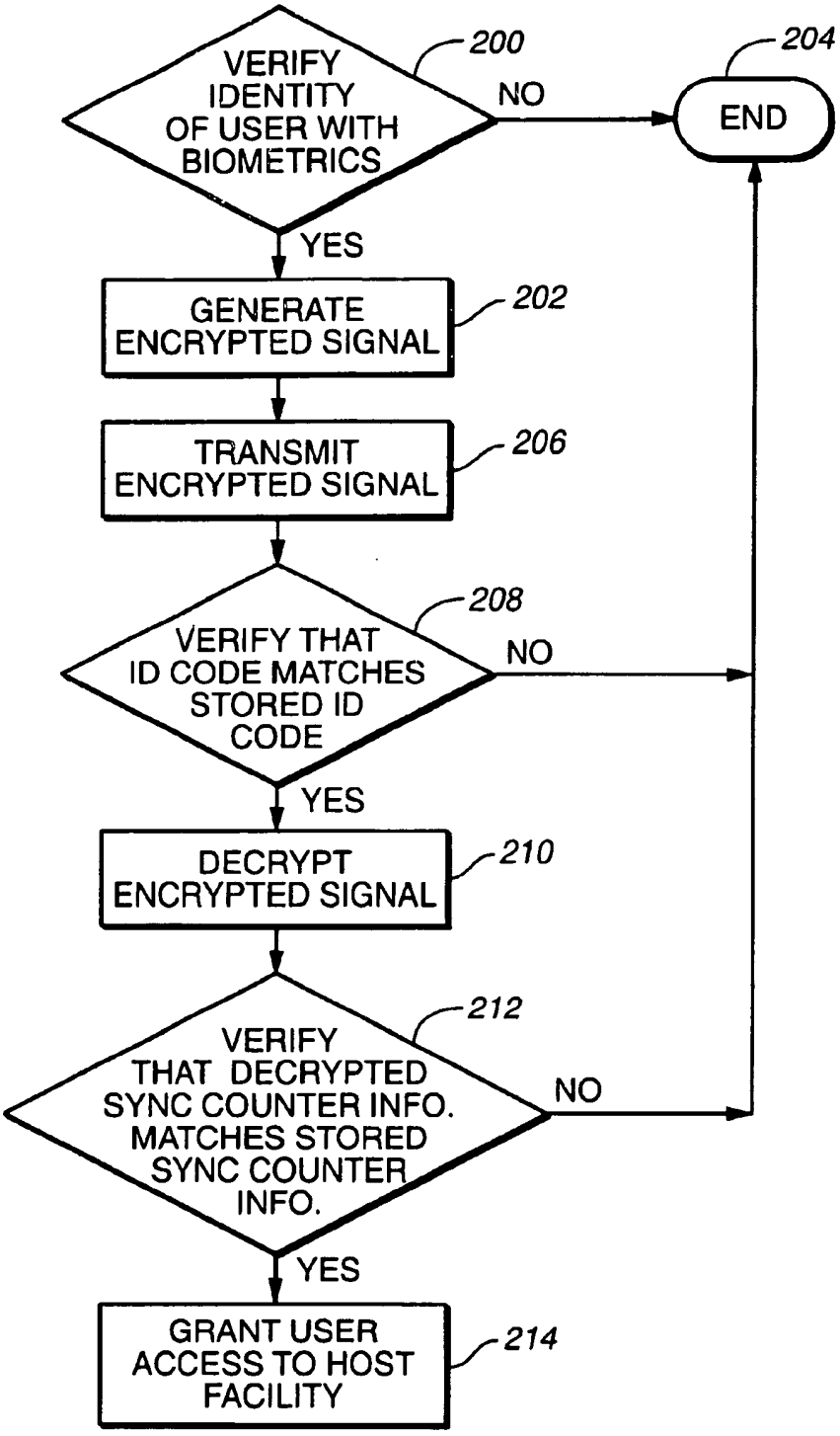

VERIFY IDENTITY OF USER WITH BIOMETRICS
200
NO
END
204
YES
GENERATE ENCRYPTED SIGNAL
202
TRANSMIT ENCRYPTED SIGNAL
206
VERIFY THAT ID CODE MATCHES STORED ID CODE
208
NO
YES
DECRYPT ENCRYPTED SIGNAL
210
VERIFY THAT DECRYPTED SYNC COUNTER INFO. MATCHES STORED SYNC COUNTER INFO.
212
NO
YES
GRANT USER ACCESS TO HOST FACILITY
214

FIG._8

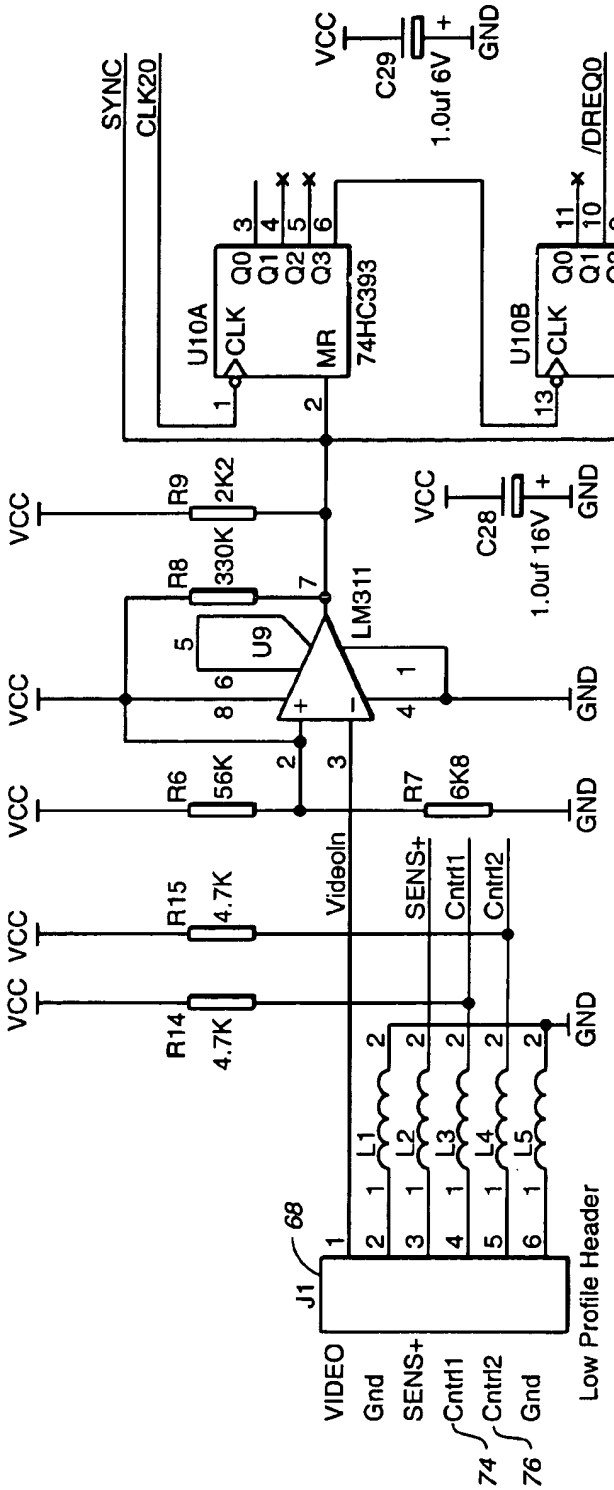


FIG._9D

FIG._9A	FIG._9B	FIG._9C
FIG._9D	FIG._9E	FIG._9F

FIG._9

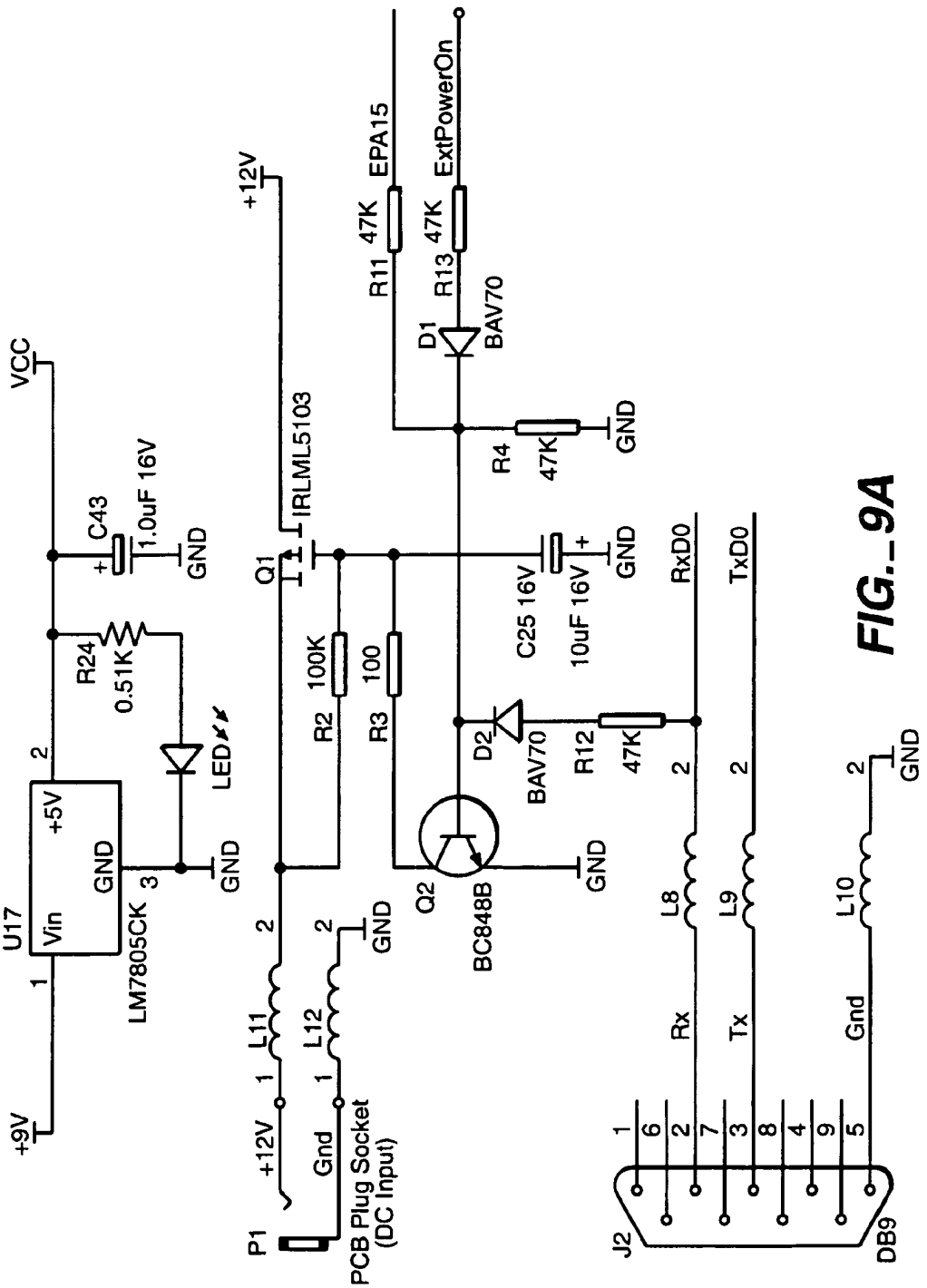

VCC
+9V
U17
Vin
+5V
GND
LM7805CK
C43
1.0uF 16V
R24
0.51K
LED
+12V
IRLML5103
Q1
R2
100K
R3
100
Q2
BC848B
R11
47K
EPA15
R13
47K
ExtPowerOn
D1
BAV70
R4
47K
C25 16V
10uF 16V
D2
BAV70
R12
47K
RxD0
TxD0
L8
L9
L10
L11
L12
P1
+12V
Gnd
PCB Plug Socket
(DC Input)
J2
Rx
Tx
Gnd
DB9

FIG._9A

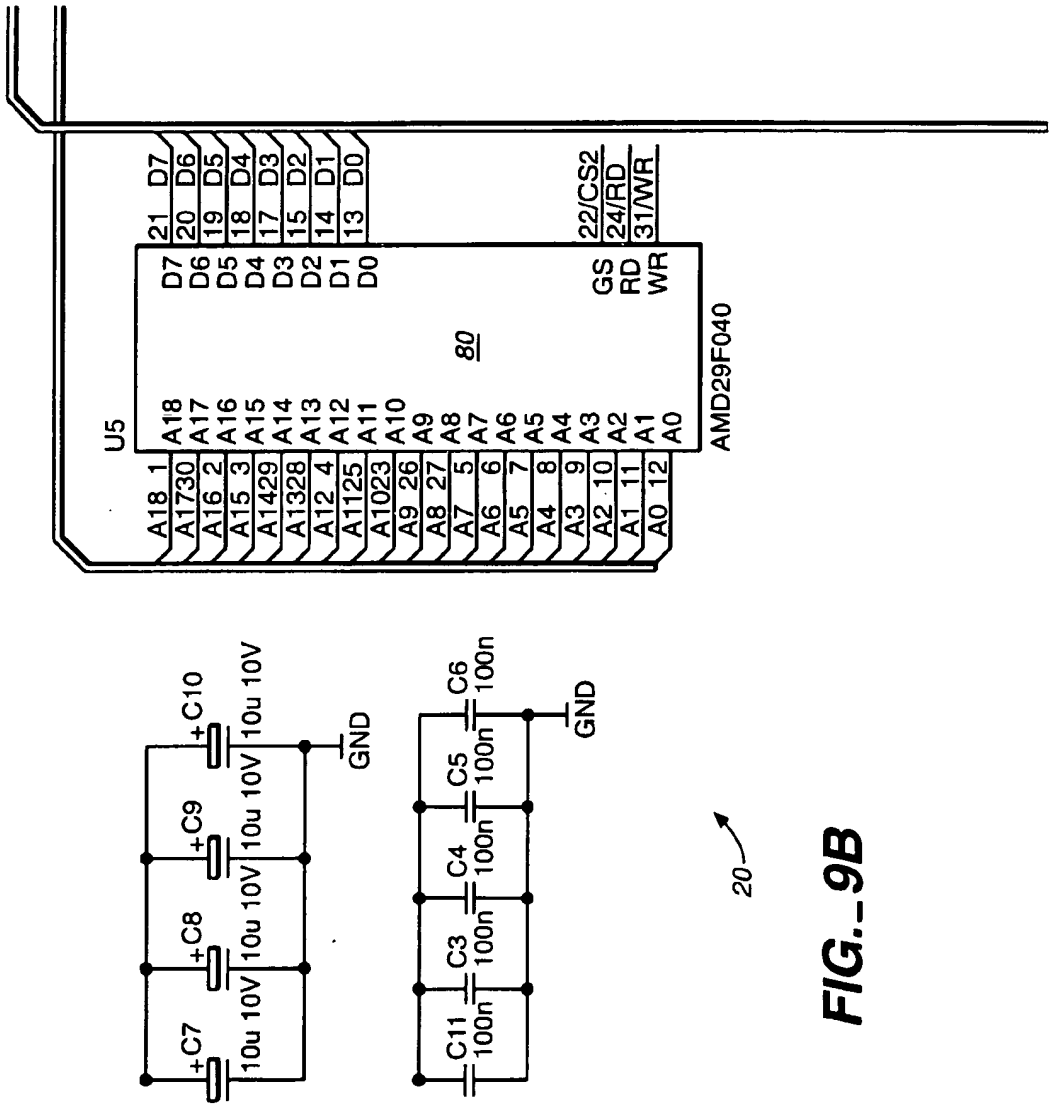

U5
AMD29F040
80
A18 1
A1730
A16 2
A15 3
A1429
A1328
A12 4
A1125
A1023
A9 26
A8 27
A7 5
A6 6
A5 7
A4 8
A3 9
A2 10
A1 11
A0 12
21 D7
20 D6
19 D5
18 D4
17 D3
15 D2
14 D1
13 D0
22/CS2
24/RD
31/WR
GS
RD
WR
+C10
+C9
+C8
+C7
10u 10V
GND
C6 100n
C5 100n
C4 100n
C3 100n
C11 100n
20

FIG._9B

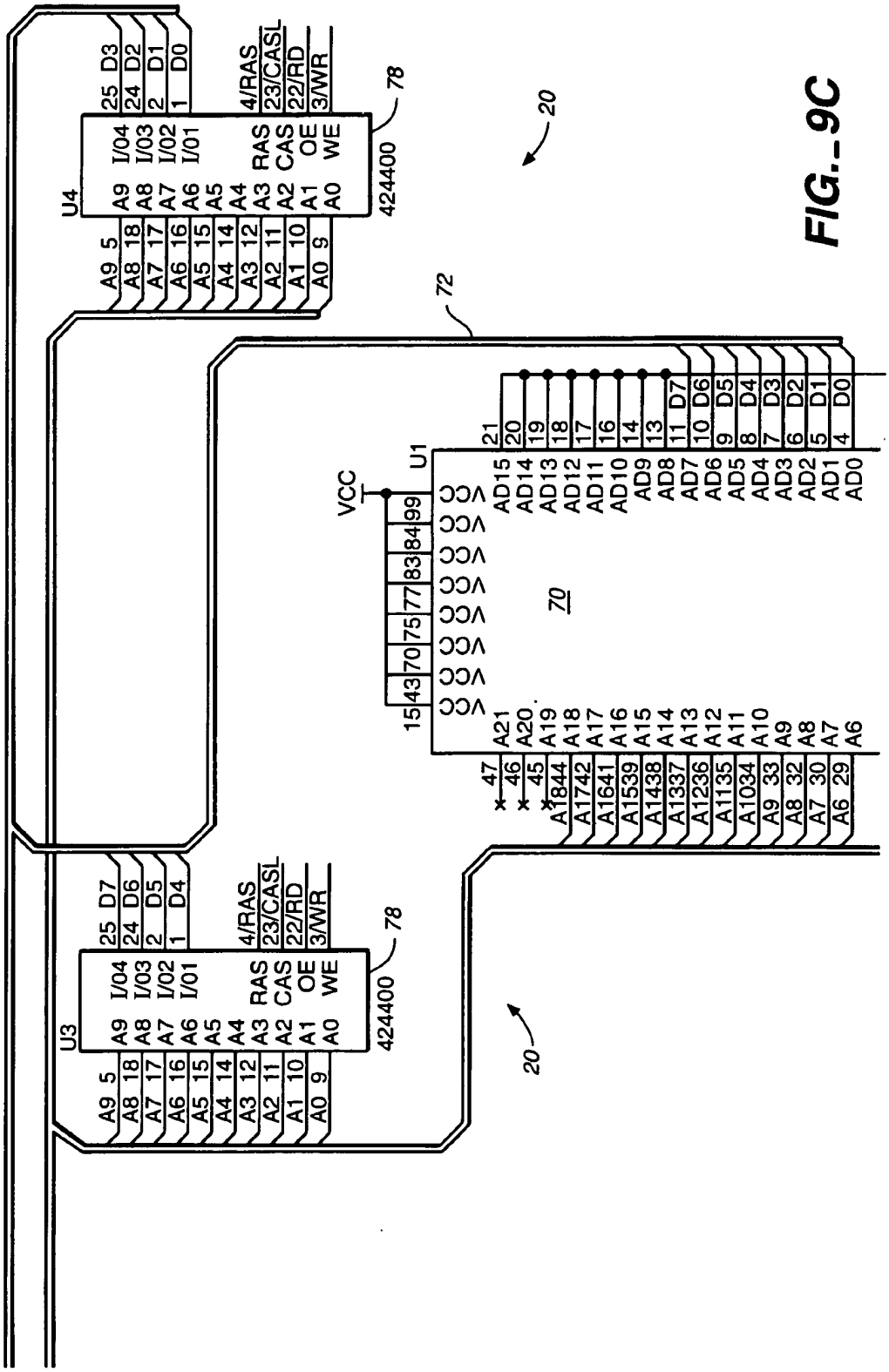

U4
U3
U1
424400
78
72
70
20
VCC
25 D3
24 D2
2 D1
1 D0
4/RAS
23/CASL
22/RD
3/WR
I/04
I/03
I/02
I/01
RAS
CAS
OE
WE
A9 5
A8 18
A7 17
A6 16
A5 15
A4 14
A3 12
A2 11
A1 10
A0 9
25 D7
24 D6
2 D5
1 D4
21 20 19 18 17 16 14 13 11 D7 10 D6 9 D5 8 D4 7 D3 6 D2 5 D1 4 D0
AD15 AD14 AD13 AD12 AD11 AD10 AD9 AD8 AD7 AD6 AD5 AD4 AD3 AD2 AD1 AD0
15 43 70 75 77 83 84 99
47 46 45 A1844 A1742 A1641 A1539 A1438 A1337 A1236 A1135 A1034 A9 33 A8 32 A7 30 A6 29
A21 A20 A19 A18 A17 A16 A15 A14 A13 A12 A11 A10 A9 A8 A7 A6

FIG._9C

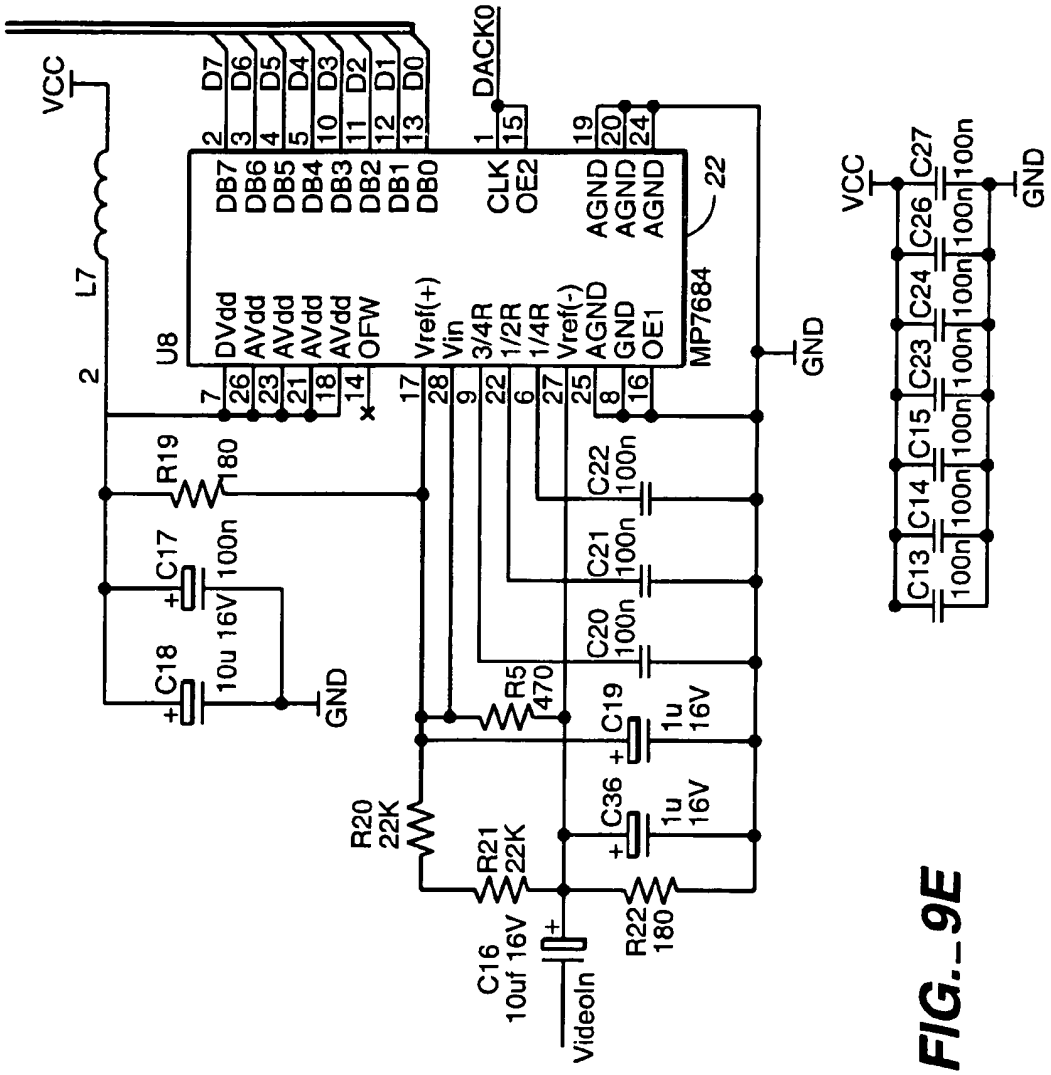
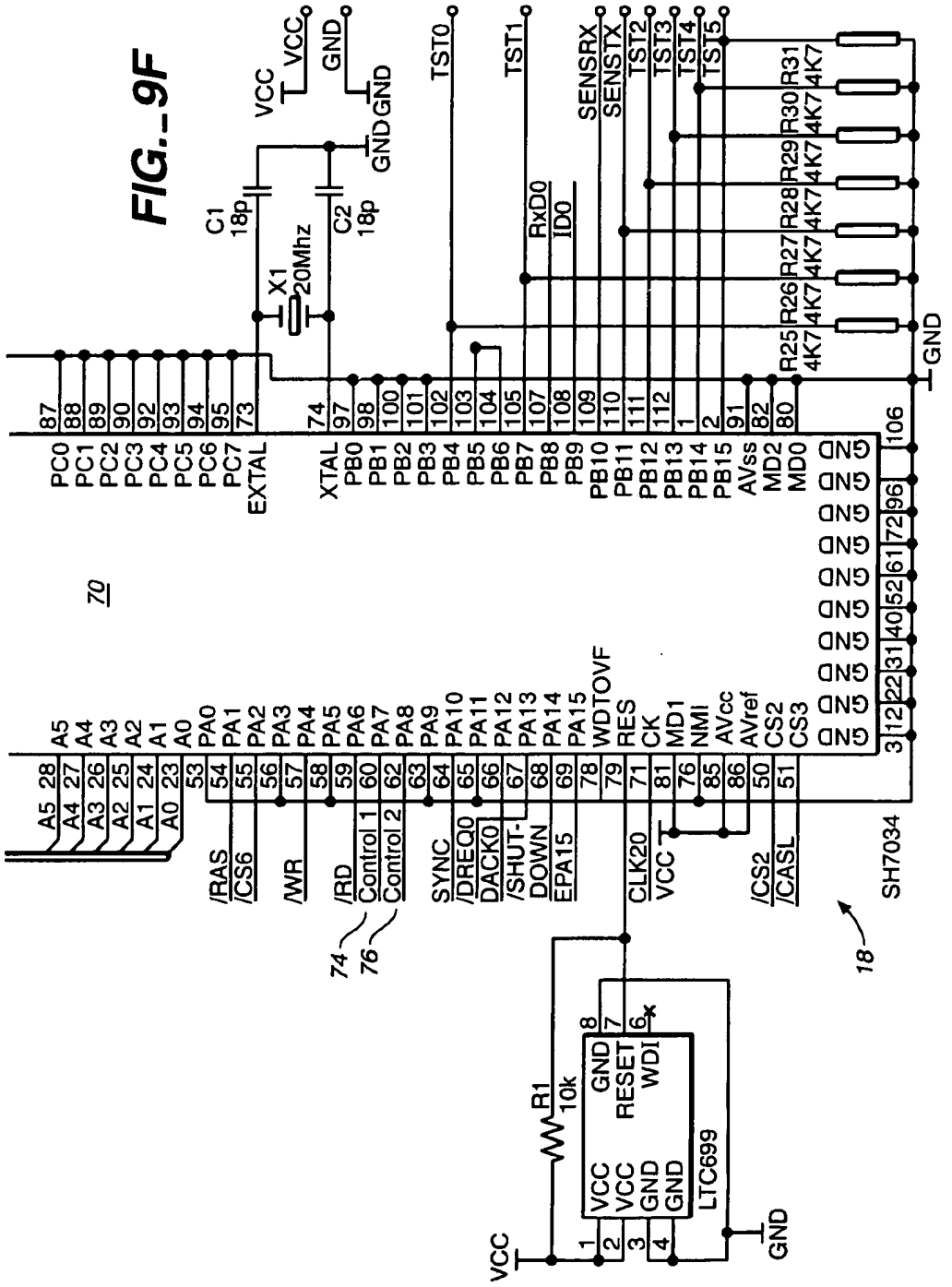

VCC
L7
2
U8
DVdd
AVdd
AVdd
AVdd
AVdd
OFW
Vref(+)
Vin
3/4R
1/2R
1/4R
Vref(-)
AGND
GND
OE1
MP7684
22
DB7
DB6
DB5
DB4
DB3
DB2
DB1
DB0
CLK
OE2
AGND
AGND
AGND
D7
D6
D5
D4
D3
D2
D1
D0
DACK0
R19 180
C17 100n
C18 10u 16V
GND
C22 100n
C21 100n
C20 100n
R5 470
C19 1u 16V
C36 1u 16V
R20 22K
R21 22K
R22 180
C16 10uf 16V
VideoIn
GND
VCC
C27
C26
C24
C23
C15
C14
C13
100n

FIG._9E

FIG._9F


70
SH7034
18
LTC699
R1
10k
C1
18p
C2
18p
X1
20Mhz
VCC
GND
TST0
TST1
SENSRX
SENSTX
TST2
TST3
TST4
TST5
RxD0
ID0
R25 4K7
R26 4K7
R27 4K7
R28 4K7
R29 4K7
R30 4K7
R31 4K7
PC0
PC1
PC2
PC3
PC4
PC5
PC6
PC7
EXTAL
XTAL
PB0
PB1
PB2
PB3
PB4
PB5
PB6
PB7
PB8
PB9
PB10
PB11
PB12
PB13
PB14
PB15
AVss
MD2
MD0
PA0
PA1
PA2
PA3
PA4
PA5
PA6
PA7
PA8
PA9
PA10
PA11
PA12
PA13
PA14
PA15
WDTOVF
RES
CK
MD1
NMI
AVcc
AVref
CS2
CS3
/RAS
/CS6
/WR
/RD
Control 1
Control 2
SYNC
/DREQ0
/DACK0
/SHUT-DOWN
EPA15
CLK20
/CS2
/CASL
A5 28
A4 27
A3 26
A2 25
A1 24
A0 23
RESET
WDI
VCC
GND

PERSONAL IDENTIFICATION SYSTEM

BACKGROUND OF THE INVENTION

The invention relates to a personal identification system employing a biometric sensor for allowing access to secure facilities.

Some security systems, such as home security systems and door locks, require a user to enter a fixed code into a device at a host facility before allowing a person access to the facility. Other systems, such as automated teller machines (ATM), require a person to submit an authorized card and also to enter a fixed code that is associated with the person's bank accounts. Automobile alarms, locks, and disabling devices, and garage door openers can be operated by pressing a button on a small remote device to transmit a coded signal to a receiving unit on the automobile or garage.

Each of these security systems can be operated by any person who is in possession of the fixed code, the card or the transmitting device, as the case may be. Therefore, each of these systems is inherently insecure. Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility. The biometric trait is a unique identifier of a person, and can be, for example, a person's fingerprint, voice pattern, iris pattern, or the like. The requesting person also enters other identifying information about himself. The measured biometric trait is compared with stored biometric data associated with the identified person and, if there is a match, the requesting person is allowed entry or access to the host facility.

In presently available biometric systems, each authorized person registers with the host facility by providing a sample of their biometric trait, for example, by having his fingerprint optically scanned into a host system data base. Each host facility must have a biometric sensor, access to the database of registered persons' biometric trait registration data, and a processing system capable of quickly searching the database and conducting the comparison to verify a person's identity. However, if the set of authorized persons is large, such a system would require a huge database to store the fingerprint images of all the authorized persons, and the identification process would become slower as the set of authorized persons increases.

SUMMARY OF THE INVENTION

According to one aspect of the invention, a portable personal identification device for providing secure access to a host facility includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof. A processing circuit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person. The processor provides a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal is indicative of the enrolled person or the device. A communication unit, including a transmitter circuit, is adapted to transmit the verification signal to a remote host system.

The communication unit is preferably adapted for remote communication with the host system via a wireless communication medium. The device can further include a display and a keypad.

The biometric sensor system can include a fingerprint sensor, a voice sensor, or any other type of biometric sensor.

The fingerprint sensor can include a platen adapted for placing a finger thereon. The fingerprint sensor can further include an optical image sensor, which may include a complementary metal oxide semiconductor (CMOS) optical sensor, a charge coupled device (CCD) optical sensor, or any other optical sensor having sufficient resolution to provide a signal indicative of a fingerprint image. In the embodiments with an optical sensor, the platen would include an optical platen, and the biometric sensor may also include a lens focusing light from the platen onto the optical sensor. The fingerprint sensor can alternatively include a direct contact sensor device, such as a capacitive sensor chip or thermal sensor chip. In these embodiments, the platen would be the surface of the sensor chip.

The processing unit can include a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal includes an encrypted signal encrypted by the encoder. In one embodiment, the encoder includes an encoding circuit, and the verification signal further includes an ID code indicative of the enrolled person or the device.

In another embodiment, the encoder comprises an encryption algorithm programmed into the processor. The encryption algorithm employs a private key indicative of the enrolled person or the device. In this embodiment, the communication unit can further include a receiver circuit. The memory can further store an ID code indicative of the enrolled person or the device. The processor unit can be further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system. The receiver circuit can be adapted to receive a host response signal transmitted by the host system in response to the ID code signal. The processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.

In either of these embodiments, the memory can be located in a removable plug-in module, and the personal identification device further includes a socket adapted to receive the module.

According to another aspect of the invention, a portable, hand-held personal identification device for providing secure access to a host facility includes a housing. A fingerprint sensor system in the housing is capable of sensing a fingerprint of a user and providing a fingerprint signal indicative thereof. The fingerprint sensor system includes a platen on a surface of the housing adapted to receive a finger. A communication unit in the housing is adapted for wireless communication with a separate host system. The communication unit includes a transmitting circuit and a receiving circuit. A slot in the housing receives a removable smart card that includes a memory. The device can be combined with the smart card. The memory in the smart card stores a fingerprint template representative of the fingerprint of an enrolled person, and an ID code and a personal encryption key being associated with the device. A processing circuit in the device is adapted to cause the ID code signal from memory to be transmitted by the transmitting circuit. The processing circuit is further adapted to cause a host response signal received by the receiving circuit signal from the host system in response to the ID code signal to be encrypted according an encryption algorithm employing the personal encryption key and to cause the encrypted host response signal to be transmitted by the transmitting

circuit only if the fingerprint signal corresponds sufficiently to the fingerprint template to verify that the user is the registered person.

According to yet another aspect of the invention, a method of providing secure access to a host facility includes the step of registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person. The method also includes receiving a first transmission comprising a first user signal at the host facility, generating and then transmitting a random number signal from the host facility only if the first user signal represents one of the stored ID codes, receiving a second transmission comprising a second user signal at the host facility, decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal, and providing access to the host facility only if the decrypted second user signal represents the random number.

According to still another aspect of the invention, a method of providing access to a secure host facility only to registered persons includes registering one or more registered persons with the host system. Registering each registered person includes storing an ID code associated only with a portable hand-held device under the control of that registered person. The method also includes transmitting an ID code signal from a portable hand-held device to a host facility of the host system. The ID code signal represents an ID code associated with the transmitting device. Other steps include generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons, and retrieving, with the host system, a public key associated with the one of the registered persons only if the ID code signal is representative of the ID code of the one the devices controlled by the one of the registered persons. Retrieving the public key can include retrieving the public key from a trusted third party. Further steps include transmitting the random number signal from the host facility to the transmitting device, and receiving the random number signal with the transmitting device. The method also includes generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of the transmitting device, and comparing, with the transmitting device, the user fingerprint signal to a fingerprint template stored in the transmitting device, wherein the fingerprint template represents a fingerprint image of a person who is enrolled with the transmitting device. Other steps include encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device, transmitting the encrypted random number signal from the transmitting device to the host facility only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, decrypting the encrypted random number signal with the host system, including employing the retrieved public key, and providing the user access to the host facility only if the decrypted encrypted random number signal represents the random number.

Transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each can include transmitting via a wireless transmission. Transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each can further include transmitting via at least one of a modem, a cable access TV line, and a computer communication medium.

In yet another aspect of the invention, a method of providing a secure function at a host facility only to a registered person includes registering a person with the host facility by storing an ID code associated only with a portable registered device controlled by the registered person, learning a synchronization counter of the registered device, storing an encryption key associated with the registered device and associating the encryption key of the registered device with the stored ID code. The method also includes generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of a portable user device, comparing, with the user device, the user fingerprint signal to a fingerprint template stored in the user device, the fingerprint template representing a fingerprint image of an enrolled person who is enrolled with the user device, and generating an access signal with the user device only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, the access signal including an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device. The method then includes transmitting the access signal from the user device to the host facility, determining, with the host facility, if the ID code in the access signal matches the stored ID code, retrieving the encryption key of the registered device if the match is successful, employing the encryption key of the registered device to decrypt the encrypted data and determine the synchronization counter of the user device, comparing the synchronization counter of the user device with the synchronization counter of the registered device, and providing the requested function represented by the button press data only if the synchronization counter of the user device matches the synchronization counter of the registered device.

In another aspect, the invention provides a method of accessing a secure host facility, including sensing a biometric trait of a user that is unique to a user with a biometric sensor system of a portable device, and providing a biometric signal indicative of the biometric trait; comparing, with the portable device, the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person; providing a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and transmitting the verification signal and an ID code signal to a remote host system, wherein the ID code signal is indicative of an ID code associated only with the portable device, and wherein the host system provides access to the secure facility in response to the verification signal only if host facility determines that personal device associated with the ID code belongs to a registered person.

The system can be employed to provide secure access to a variety of different types of host facilities. The system can be used to replace security systems employing key card entry, fixed code entry, or a combination of key card and fixed code entry, which are currently employed, for example, with ATM's, gate and garage door openers, burglar alarm systems, point of sale (POS) devices, hotel room locks, and

the like. The system can also be configured for use with automotive remote key entry (RKE) systems, automotive alarm systems, and automotive immobilizers.

The personal identification device and system of the invention has several advantages. The system is very private. Persons' biometric data, such as a fingerprint, are not stored in a central database, as with prior art systems using fingerprint identification for security. An electronic template of a user's fingerprint is stored only with their own personal identification device, and is used only for verifying the user's fingerprint. In the embodiment with two-way communication, the host facilities store only an ID code and a public key for each registered person. The ID code may be the serial number of the device, and the public key can be retained by a trusted third party. The private key used by the device is never disclosed.

The personal identification device is compact, being about the same size as an electronic pager. With advances in technology, it could be made even smaller. The personal identification device can be configured such that all the information that is associated with the user, i.e., the ID code, the personal encryption key, and the fingerprint template, is stored in a smart card, which can be transferred between identical devices having the image capture electronics, processing circuit, communication module and power supply. This enables the user to switch devices when one is worn out or broken without having to reregister.

The host system can be installed at host facilities with a minimal expenditure compared with current systems employing fingerprint identification for security. The biometric sensor is installed in each personal identification device, rather than with the host facility. This configuration also makes retrofitting existing security systems for use with the personal identification device a relatively simple procedure. The point of contact is with the personal identification device, which makes the present system more feasible for use at exposed, public locations, such as with automated teller machines, parked automobiles, and gate entries, where the weather and vandalism can be problems. This also makes the system of the invention more sanitary than other systems that require a person to operate a public terminal, keypad, or fingerprint scanner.

Because each user carries his own fingerprint template in the personal identification device, users can "roam" to many different applications and host facilities without the need to enroll the template at each site. They only need to register prior to use. This can be done over the phone or over computer communication lines, such as the Internet, if only medium level security is required.

The user has total control over the procedure for accessing a host facility. The ID cannot be read unless the user presses the fingerprint reader. The random number transmission and the encrypted random number transmission cannot be "scanned" as the random numbers are different each time access to a host facility is requested. The personal identification device can be used in conjunction with conventional telephone lines or computer network communication lines without any risk of theft.

Personal identification devices could be sold via any retail outlet, for example, as a shrink wrap product. As the units are manufactured with unique ID codes and private keys there is no need to control the sale in any way.

Unlike prior art biometric identification systems, the user is already enrolled by the first use of the personal identification device. This completely eliminates the delays and problems associated with enrolling large numbers of users and storing each user's biometric data.

BRIEF DESCRIPTION OF THE DRAWING

FIG. **1** is a block diagram of a security system according to the invention.

FIG. **2** is a block diagram of another embodiment of a security system according to the invention.

FIG. **3**. is a perspective view of a personal identification device according to another feature of the invention.

FIGS. **4A**, **4B**, **4C**, and **4D** are respective front, side, top and bottom views of an embodiment of a personal identification device.

FIGS. **5A** and **5B** are respective front and side views of another embodiment of a personal identification device.

FIG. **6** is a front view of a third embodiment of a personal identification device.

FIG. **7** is a flow diagram illustrating an embodiment of a method of accessing a host facility with a personal identification device.

FIG. **8** is a flow diagram illustrating another embodiment of a method of accessing a host facility with a personal identification device.

FIG. **9** is a schematic diagram of an embodiment of the processor unit.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. **1**, a security system **2** provides access to one or more secure host facilities **4** only to registered persons. A host facility **4** may be a bank, a store, a military base, a computer system, an automobile, a home security system, a gate, or any other facility where it is desired to restrict access to selected individuals. Each registered person uses a battery powered, portable personal identification device (PID) **6**, which communicates with a communication unit **8** located at each host facility **4**. PID **6** is small enough to carry on ones person, being similar in size to a hand-held pager. An example of a PID **6** is shown being held in the palm of a man's hand **10** in FIG. **3**.

PID **6** includes a biometric sensor. In the described embodiment, a biometric sensor **11** includes an optics unit **12** having a CMOS optical sensor imaging device **14**, and an exposed optical platen **15**. Imaging device **14** can also be a CCD imaging device. A lens (not shown) may also be used to focus an image from a surface of platen **15** onto imaging device **14**. PID also includes a processing unit **16**. Processing unit **16** includes a processor circuit **18**, an external memory **20** and may include an analog-to-digital converter circuit (A/D) **22**. Some CMOS optical sensors provide a digital output signal, which eliminated the need for A/D **22**. PID **6** further includes a communication unit **24**, which has a transmitter module **28** and a receiver module **26**.

Memory **20** stores information that is specific to processing unit **16**. Memory **20** stores an ID code that is set in PID **6** by the manufacturer. The ID code of a device, which may be the device serial number, is unique to each device. Memory **20** also stores a fingerprint template that is generated by processing unit **16** from a fingerprint image signal provided by optics **12** unit when an individual first enrolls into PID **6**, as will be described in detail below. That fingerprint image signal is representative of an image of a fingerprint of the enrolled individual. The fingerprint template is a data set that is representative of features of the enrolled individual's fingerprint. The fingerprint template is normally not changed once it is established in memory **20**. In some embodiments, PID **6** may include a serial port (not

shown), which can be used to plug into a computer to update or change the fingerprint template. For security purposes, PID **6** would be used to perform an identification verification before allowing such a change.

Processing unit **16** also includes an encryption algorithm incorporated into an encoder **23**. In the embodiment illustrated in FIG. **1**, the encryption algorithm is programmed into processor circuit **18**. A private key that is stored in memory **20** is used with the encryption algorithm for encryption. The private key can be set into memory by the manufacturer, and is specific to each PID **6**. Different PIDs **6**, which have different processing units **16**, will typically have different private keys. The encryption algorithm, on the other hand, can be the same for all PID's **6**.

Host facility **4** is part of a host system **30**. Host system **30** will typically be bank ATM systems, point of sale systems, and the like. Host system **30** also includes a host processing unit **32**, which has a processor circuit **34** and memory **36**. Communication unit **8** in host facility **4** includes a receiver module **38** and a transmitter module **40**. Host processing unit **32** may be located with host facility **4**, or may be located at a remote location, where it may also serve other host facilities **4** in a distributed network **42**.

Memory **36** stores ID codes of enrolled individuals who have registered with host system **30**. Memory **36** also stores public keys associated with respective ones of the stored ID codes. By employing the correct public key associated with a specific ID code, host processor circuit **34** can decrypt a signal that has been encrypted according to the encryption algorithm and personal key associated with the specific ID code, in a manner known in the encryption arts. The public key can also be stored with a trusted third party **39**, which provides this service for several host systems in a known manner.

Signals **41** can be transmitted between PID **6** and host facility via any wireless transmission method. Transmission can be via RF, infrared, induction, sound, or the like. In this embodiment, PID communication unit **24** and host communication unit **8** will normally have a short transmission range of approximately a meter or less; however, longer ranges can be used as well. Hard-wire transmission methods can also be employed, either alone or in combination with a wireless transmission method. For example, transmission can employ dial tone modulation frequency (DTMF) (tone transmission) via a conventional phone system, employ a cable TV line in conjunction with the cable remote control system, or employ a computer communication medium, such as the Internet or a private network. PID **6** can employ more than one transmission/reception mode, such as, for example, an RF and a DTMF unit.

In another embodiment of a security system **2A**, shown in FIG. **2**, a PID **6A** includes most of the features of PID **6** described above with reference to FIG. **1**, with some significant differences. Note that features that system **2** has in common with system **2A** are labeled with the same reference numerals in FIGS. **1** and **2**, which convention is continued in the remainder of the FIGS. and in the following description. One difference is that communication module **24A** lacks receiver module **26**. Also, encoder **23A** includes an encoder chip, for example, the HSC200 or HSC300 KeeLoq® Code Hopping Encoder, available from Microchip Technology, Inc. of Chandler, Ariz., that contains the encryption algorithm. Security system **2A** includes a host facility **4A** in which host processing unit **32A** is located at the same site as host facility **4A**. Host system communication unit **8A** includes a receiver module **38**, but does not include a transmitter module.

The embodiment illustrated in FIG. **2** will typically be employed with systems such as garage door openers, automobile security systems, door locks, and the like. As such, PID communication module **24A** will have a longer transmission range than communication module **24** in the embodiment illustrated in FIG. **1**.

Encoder **23A** includes an ID code, which may be a serial number of encoder **23** or PID **6A**. Encoder **23A** also includes a synchronization counter, an encryption key and an encryption algorithm that employs the encryption key. Host system **4A** must "learn" the ID code and the synchronization counter for each PID **6A** which is used to access a function of host system **4A**. Host system **4A** must also know the encryption key.

Referring now to FIGS. **4A–4D**, one embodiment of a PID **6B**, which includes all the features also shown in FIG. **1**, includes a housing **44** similar in size to a personal pager or a small cellular telephone. A front side **46** includes a keypad **48** for entering data and commands, and a liquid crystal display **50** for displaying data being entered with keypad **48** and for displaying status signals to the user. Keypad **48** can be eliminated in some models where programmability is not required. Platen **15** is located at the top of PID **6B**, and is contoured for a finger. Platen **15** is also slightly recessed in the housing to provide some protection from scratching. A back side **56** of PID **6B** includes a battery cover (not shown) and apertures for a DTMP speaker (not shown). A serial port can be included under the battery cover.

Housing **42** includes a slot **52** for receiving a smart card **54**, which is shown in shadow being fully inserted into slot **52** in FIG. **4A**. Smart card **54** includes external memory **20**, and can be removed from one housing **42** and used in a new housing **42**. Because memory **20** contains all the personal information, i.e., the private key, the ID code, and the fingerprint template, the smart card can be used with a different PID housing **42** without having to re-enroll the user or reregister any user information with host systems. Some models in which memory **20** is hard-wired inside housing **42** would not include smart card slot **52**.

FIGS. **5A** and **5B** illustrate an embodiment of a PID **6C** in which keypad **48** and smart card slot **52** are not included. PID **6C** does, however, include platen **15**, display **50**, and a belt clip **58**, which could be included in any model.

FIG. **6** illustrates an embodiment of a PID **6D** which is structured similar to the embodiment illustrated in FIG. **2**, for uses such as a garage door opener or automobile security system. PID **6D** includes platen **15** at the top of housing **42**, and three function buttons. For an automobile security system the function buttons can be a driver door button **60**, a trunk button **62** and an alarm button **64**. Buttons **60**, **62**, and **64** can be adapted for use with other host systems having different functions.

Optics unit **12** can be an image sensor module available from Fingerscan PTY Ltd (an Identix company), of Sydney, Australia, as part of their F3 OEM Kit. The entire F3 OEM Kit manual, published in 1998, is incorporated herein by reference. Platen **15** and imaging device **14** have a usable area of about 16 mm×18 mm. Imaging device **14** in the F3 OEM kit is a CMOS device that provides a video output comprising an analog fingerprint image signal representing an image of a finger placed on platen **15**. The fingerprint image signal is communicated to processing unit **16** via a six-wire connector **68**, which is shown in a circuit diagram illustrated in FIG. **9**.

Most of processing unit **16** is also included in the F3 OEM Kit. Referring again to FIG. **9**, processor circuit **18** includes

an SH7034 32-bit RISC microprocessor **70**, made by Hitachi of Japan. Microprocessor **70** communicates over an 8-bit data bus **72** with external memory **20** and A/D **22**, and over control lines **74**, **76** with optics unit **12**. The SH7034 microprocessor **70** has a 64 KB internal programmable read only memory (PROM) engine and an internal 4 KB static random access memory (SRAM).

In the PROM resides a Fingerscan Biometrics Engine (FBE), which includes algorithms for capturing and processing fingerprint image signals. These algorithms allow a finger image of approximately 140 Kbytes to be converted into a finger model, or template, of approximately 120 bytes. This size saves memory and improves the speed of processing by decreasing the time it takes to transfer finger models to and from the internal memory. The FBE includes special instruction sequences to optimize the following operations: image capture and background rejection; video signal filtering and digitizing; template matching; finger presence detection; false finger detection; and power on self test.

A/D **22** converts the analog video signal from optics unit **12** into digital data that is stored in memory for subsequent use by processor circuit **18**. Memory **20** also stores the finger template of the user who is enrolled in PID **6**, and also stores custom written code. Microprocessor **70** controls and has access to 1 Mbyte in DRAM **78** and 512 Kbytes of external flash memory in PROM **80**. DRAM **78** includes two NEC 424400 chips, and PROM **80** is an AMD 29F040 chip.

In one embodiment of communication unit **24**, transmitter module includes an induction loop data link, which is configured as a short-range (<0.5 m) wireless modem, operating at 1200 Baud, at 70 KHz carrier frequency, using amplitude shift keying modulation. The protocol is half duplex, carrier detect multiple access (modified aloha) and the software includes a CRC 16 packet error correction method. A processor included in transmitter module is based on a PIC16C72 device. The transmit current is typically 1 mA.

In the embodiment illustrated in FIG. **9**, encoder **23** resides in code programmed into processing circuit **18**. However, as discussed above, other embodiments may base encoder **23** on a dedicated encoder chip, such as the HSC200 or HSC300 KeeLoq® Code Hopping Encoder. A PID may include encryption code residing in processor circuit **18** and also include an encoder chip so that PID can combine the functions of the embodiments illustrated in FIGS. **1** and **2** in a single unit. These encoder chips combine a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and 6 information bit to create a 66-bit transmission stream. The length of the transmission eliminates the threat of code scanning, and the code hopping mechanism makes the transmission unique, thus rendering code capture and resend schemes useless.

An owner of PID **6** must first "enroll" into the unit. Enrollment is the process of scanning a finger to create an image which is stored as a fingerprint template in memory **20**. The user enrolls on the unit by removing the "packing" cover and placing a thumb or finger on platen **15**. PID can be configured to automatically start the enrollment routine with this action. Enrollment takes approximately 7 seconds. The resultant template is stored in memory **20**. Ideally, PID **6** is configured to enable a user to enroll one finger on each hand so that, if the user injures the finger they usually use for verification, an alternate image is available.

Enrollment preferably permits the user several attempts to check and test the operation on the verify. Instructions and queries would be indicated, for example, by display **50** in this mode (see FIG. **4A**). Until the user accepts the enrollment the unit will not transmit signals in any way but will allow any number of attempts to re-enroll and verify (test) the operation. Once committed there is no going back or editing.

If the enrollment is be stored on a removable smart card **54** (see FIG. **4A**) along with the ID code and private encryption key files, these would not be accessible to other devices. It allows users to swap their PID **6** and retain their enrolled identifying data on smart card **54**, while using other PIDs **6**. This is the same process used in digital portable telephones today. A user can take the SIM card out of the telephone and swap phones without any security issues.

Verification is carried out when a user places his finger on platen **15**, or presses a verify button if included in PID **6**. In the embodiment illustrated in FIG. **4A**, the verify button can be a dedicated button, such as the # button **55**, or could be any other button or sequence of buttons. Each time the user places his or her finger on platen **15** (or presses the verify button and places their finger on platen **15**) the optics unit **12** creates a fingerprint signal indicative of the fingerprint image of the user's finger on platen **15**. The fingerprint signal is compared to the stored fingerprint template. If the two are significantly similar, the user's identity is verified to be the enrolled person. Verification takes about 1 second or less once the fingerprint template has been retrieved from storage. The user's fingerprint is always verified with the fingerprint template to allow the use of the encryption key.

In programmable PID's, verification for individual users can be set at various threshold levels to account for users who may have very fine, worn or damaged fingers. In this event the ease of use can be enhanced by reducing their verification threshold. Verification threshold can be set at the time of enrollment.

Once the owner or person controlling the unit is enrolled, the unit can then be "registered" with numerous organizations. The host organization is only interested in knowing the ID code and the public encryption key.

The operation of security system **2** illustrated in FIG. **1** is different from the operation of security system **2A** illustrated in FIG. **2**. The operation of the embodiment illustrated in FIG. **1** will be described first.

In the first embodiment illustrated in FIG. **1**, each of PID **6** and host facility **4** include transmit and receive functions. A communication from PID **6** to host system **30** is encrypted according to an encryption algorithm that employs a private key in encrypting and a public key to decrypt. The public encryption key is associated with PID **6** and therefore also with the enrolled person. The private encryption key is stored or loaded into PID **6** at registration time or at manufacture. When a user registers with each host system **30**, the user provides the user's ID code and public key to host facility **4** as part of the user's account record. The public key can be stored by the host system. Alternatively, the user provides the public key to a central authority (trusted third party **39**) with which host system **30** can communicate.

Referring now to FIG. **7**, a user of PID **6** approaches host facility **4**, e.g., an ATM (**100**). As PID **6** reaches the range of the host facility's receiver module **38**, the microprocessor is "powered up." The user may have to select a transmission mode that matches that of host system **30**, if more than one transmission mode is available on PID **6**. Processor circuit **18** causes transmitter module **28** to transmit the ID code signal without encryption (**102**). This is received by host receiver module **38** and passed on to host processing unit **32** (**104**). Host processing unit **32** verifies that the received ID

code signal represents a registered ID code (106). If the verification fails, then the access process ends (108). If the ID code is verified, then the account or user information is located, including the public encryption key associated with the registered ID code (110). The public encryption key may have to be retrieved from a remote source, such as a central authority. A large random number is also generated by host processing unit 32 (112), and is passed on to transmitter module 40. Transmitter module 40 transmits a random number signal indicative of the random number to PID 6 (114). Receiver module 26 passes the random number signal to processing unit 16 (116). PID 6 performs a user verification (118). If the verification fails, the process ends (108). Alternatively, PID 6 can display a prompt to try again. If the user's identity is successfully verified as a match with the enrolled person based upon a comparison of the stored fingerprint template and a fingerprint image signal generated when the user places his finger on platen 15, the private encryption key associated with PID 6 is used to encrypt the random number according to an encryption algorithm (120). Processing unit 16 causes transmitter module 28 to transmit a signal representing the encrypted random number to host system 30 (122), where host processing unit 32 uses the public encryption key to decrypt the encrypted random number (124). Host processing unit 32 then determines if the decrypted random number matches the random number (126). If this is successful, then the user is granted access to the host facility (128). If this verification fails, the user is denied access (108). The step of verifying the identity of the user with the biometrics (118) can be performed at other junctures of the process, such as prior to transmitting the ID code signal (102), however, it must be carried out before encrypting the random number (120).

Hardware for host system 30 can include a small communication unit 8 with a sensor, such as an RF antenna. Processor circuit 34 can include a CPU to generate a random number, to verify the ID code received from PID 6, to decrypt the encrypted random number received from PID 6, and to compare the decrypted random number with the earlier generated random number.

As these transmissions are random, there is no possibility of scanning or tracking the codes other than to find the original ID code, which is effectively of no real use. The random number generators are such that they will always produce unique codes.

If a host system 30, such as a bank, a store, or a credit card company, implements this system, it would have the users register by presenting themselves with their PID 6 and the required personal identification papers, which is no different than current methods of obtaining a bank card to access accounts with an ATM. The bank or other host system 30 would ask the user to complete a verify on their PID 6 and read the ID code and test the send and receive of the encryption codes. This would establish the public key with the bank and confirm the private key in PID 6. The user is now ready to use the system. Note that the bank does not have the user's fingerprint template—it only has the ID code and the public encryption key. Therefore there is no privacy issue regarding release of the user's fingerprint template.

After the user registers, verification is as described above. From the bank's point of view, the ATM (for example) commences normal operation. The user, instead of entering a bank card and a personal identification number (PIN), may simply press a verify pad or button on their PID 6 while placing their finger on platen 15. The ATM receiver reads the ID code, and if the code is valid generates a large random number, and transmits the number to the user's PID 6. If the validation is successful, PID 6 then encrypts the random number using the private encryption key according to the encryption algorithm, and transmits the result back. The bank system checks the result using the public encryption key and confirms the correct identity of the user. The transaction proceeds.

The bank's ATM will typically be connected to the Bank central system via network 42. Network 42 can be used for transmitting signals between the ATM and the bank central system where the CPU and data bases may be located.

The private encryption key can only be used after a verify, host system 30 knows the ID is correct as the key is unique to that user. Therefore, only that user could be carrying the reader. The key may well be installed during manufacture but only released after the unit is loaded with a template.

In a second mode of operation, typically used in car alarm systems and the like, PID 6A is configured as shown in FIG. 2 to transmit, and host facility 4A is configured to only receive. Receiver module 38 is a standard automobile or garage door type of installation. There is no special adaptation other than the required alarm or immobilizer installation. These systems include a "learn" mode, which is used to program in the new system. In learning a registering person's PID 6A, the host system 4A learns the ID code, the synchronization counter timing, and the encryption key of that PID 6A. This process is essentially the same as the learning process for many current model garage door openers, automobile security systems and the like.

Referring to FIG. 8, to obtain access to host facility 4A, the user activates PID 6A by placing a finger on platen 15. PID 6A performs a user verification from the internally stored fingerprint template (200). If the verify succeeds, processing unit 16A causes encoder 23A to generate an encrypted signal (202). If not successful, the process ends (204). The encrypted signal includes the unencrypted ID code of PID 6, encrypted synchronization counter information and unencrypted function button information. The encryption employs the encryption key resident in encoder 23A. Transmitter unit 28 then transmits the encrypted signal to host facility 4A (206). Host facility 4A than passes the encrypted signal to host processing unit 32A, which checks the ID code for a match with the ID code of a registered user (208). Typically, there will be only a small number of registered users for car lock and garage door systems, and each may have the same ID code and encryption key. If there is no match, then the process ends (204). If there is a match, host processing unit 4A retrieves the stored encryption key and decrypts the encrypted portion of the received encrypted signal (210). Host processing unit then verifies that the synchronization counter information in the decrypted signal matches stored synchronization counter information in memory 36 (212). If the synchronization counter information does not match the stored information, then the process ends (204). If the synchronization counter information matches the stored information, then the user is granted access to host facility 4A (214). The access granted is determined by the function button information contained in the encrypted signal.

In both embodiments, the PID unit can be set in a low power "StandBy" or "Off" function, or could be powered on by the action of pressing the platen.

There are a large number of alternative applications. For example, a hotel could employ the invention in a door lock security system. A hotel registrant would be register his PID with the hotel. The hotel would identify the user's ID code to the lock on his room's door. A member of the hotel staff

would carry a master PID which would configure the door to that PID and some other master PID for hotel staff. There would be no need for a hard wired communications system to each door unless central control is required.

The biometric sensor **11** may include a direct contact device instead of an optic sensor unit **12**. Direct contact capacitive chip fingerprint sensors can be obtained from SGS Thomson Microelectronics, of Phoenix Ariz., from Veridicom, Inc., of Santa Clara Calif., and from Harris Semiconductor, of Melbourne, Fl. A direct contact thermal sensor may also be used for fingerprint sensing.

Other embodiments are within the scope of the claims.

What is claimed is:

1. A method of providing secure access to a host facility, comprising:

registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person;

receiving a first transmission comprising a first user signal at the host facility;

generating and then transmitting a random number signal only if the first user signal represents one of the stored ID codes;

receiving a second transmission comprising a second user signal at the host facility;

decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal; and

providing access to the host facility only if the decrypted second user signal represents the random number.

2. A method of providing access to a secure host facility only to registered persons, comprising:

registering one or more registered persons with the host system, wherein registering each registered person includes storing an ID code associated only with a portable hand-held device under the control of that registered person;

transmitting an ID code signal from a portable hand-held device to a facility of the host system, wherein the ID code signal represents an ID code associated with the transmitting device;

generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons;

retrieving, with the host system, a public key associated with the one of the registered persons only if the ID code signal is representative of the ID code of the one the device controlled by the one of the registered persons;

transmitting the random number signal from the host facility to the transmitting device;

receiving the random number signal with the transmitting device;

generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of the transmitting device;

comparing, with the transmitting device, the user fingerprint signal to a fingerprint template stored in the transmitting device, the fingerprint template representing a fingerprint image of a person who is enrolled with the transmitting device;

encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device;

transmitting the encrypted random number signal from the transmitting device to the host facility only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person;

decrypting the encrypted random number signal with the host system, including employing the retrieved public key; and

providing the user access to the host facility only if the decrypted encrypted random number signal represents the random number.

3. The method of claim **2**, wherein retrieving the public key includes retrieving the public key from a trusted third party.

4. The method of claim **2**, wherein transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each includes transmitting via a wireless transmission.

5. The method of claim **2**, wherein transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each includes transmitting via at least one of a modem, a cable access TV line, and a computer communication medium.

6. A method of providing a secure function at a host facility only to a registered person, comprising:

registering a person with the host facility by storing an ID code associated only with a portable registered device controlled by the registered person, learning a synchronization counter of the registered device, storing an encryption key associated with the registered device and associating the encryption key of the registered device with the stored ID code;

generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of a portable user device;

comparing, with the user device, the user fingerprint signal to a fingerprint template stored in the user device, the fingerprint template representing a fingerprint image of an enrolled person who is enrolled with the user device;

generating an access signal with the user device only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, the access signal comprising an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device;

transmitting the access signal from the user device to the host facility;

determining, with the host facility, if the ID code in the access signal matches the stored ID code;

retrieving the encryption key of the registered device if the match is successful;

employing the encryption key of the registered device to decrypt the encrypted data and determine the synchronization counter of the user device;

comparing the synchronization counter of the user device with the synchronization counter of the registered device; and

providing the requested function represented by the button press data only if the synchronization counter of the user device matches the synchronization counter of the registered device.

7. A method of providing secure access to a host facility, comprising:

registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person;

receiving a first wireless transmission comprising a first user signal at the host facility from a portable hand-held device under the control of a registered person;

generating and then wirelessly transmitting a random number signal only if the first user signal represents one of the stored ID codes;

receiving a second wireless transmission comprising a second user signal at the host facility from the portable hand-held device;

decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal; and

providing access to the host facility only if the decrypted second user signal represents the random number.

8. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof;

a processing unit responsive to the biometric signal, being adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person, and to provide a verification signal; and

a communication unit, including a transmitter circuit, adapted to transmit the verification signal to a remote host system;

wherein the processing unit includes a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal includes an encrypted signal encrypted by the encoder;

wherein the encoder comprises an encryption algorithm, and wherein the encryption algorithm employs a private key indicative of the enrolled person or the device; and

wherein the communication unit further includes a receiver circuit, wherein the memory further stores an ID code indicative of the enrolled person or the device, wherein the processing unit is further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the remote host system, wherein the receiver circuit is adapted to receive a host response signal which is transmitted by the remote host system only if the ID code signal matches an ID code stored at the remote host system, and wherein the processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the remote host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.

9. The personal identification device of claim 8, wherein the biometric sensor system includes a fingerprint sensor.

10. The personal identification device of claim 9, wherein the fingerprint sensor includes a platen adapted for placing a finger thereon.

11. The personal identification device of claim 10, wherein the fingerprint sensor further includes an optical image sensor.

12. The personal identification device of claim 8, wherein the biometric sensor system includes an optical image sensor.

13. The personal identification device of claim 12, wherein the optical image sensor comprises a CMOS chip.

14. The personal identification device of claim 8, wherein the encoder comprises an encoding circuit, and wherein the verification signal further comprises an ID code indicative of the enrolled person or the device.

15. The personal identification device of claim 8, wherein the memory is located in a removable plug-in module, the personal identification device further comprising a socket adapted to receive the module.

16. The personal identification device of claim 8, wherein the communication unit further includes a receiving circuit being adapted to receive a host response signal from the host system.

17. The personal identification device of claim 8, wherein the communication unit is adapted for remote communication with the host system via a wireless communication medium.

18. The personal identification device of claim 8, further comprising a display.

19. The personal identification device of claim 18, further comprising a keypad.

20. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof;

a processing unit responsive to the biometric signal, being adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and

a communication unit, including a transmitter circuit, adapted to transmit the verification signal to a remote host system;

wherein the biometric sensor system includes a fingerprint sensor and wherein the biometric trait is a fingerprint;

wherein the communication unit further includes a receiver circuit adapted to receive a signal transmitted by the remote host system;

wherein the processing unit includes memory to store an ID code associated only with the device, a personal encryption key associated only with the device, and the biometric data;

wherein the processing unit is further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system, wherein the receiver circuit is adapted to receive a host response signal which is transmitted by the remote host system only if the ID code signal matches an ID code stored at the remote host system, and to employ the encryption algorithm and the private encryption key to

create the verification signal by encrypting the host response signal.

21. The personal identification device of claim 20, wherein the memory is located in a removable plug-in module, the personal identification device further comprising a socket adapted to receive the module.

22. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a housing;

a fingerprint sensor system capable of sensing a fingerprint of a user and providing a fingerprint signal indicative thereof, the fingerprint sensor system including a platen on a surface of the housing adapted to receive a finger;

a communication unit in the housing being adapted for wireless communication with a separate host system, including a transmitting circuit and a receiving circuit;

a processing circuit; and

a slot in the housing for receiving a smart card that includes a memory;

wherein the memory in the smart card stores a fingerprint template representative of the fingerprint of an enrolled person, and an ID code and a personal encryption key being associated with the device, wherein the processing circuit is adapted to cause an ID code signal indicative of the ID code from memory to be transmitted by the transmitting circuit, and wherein the processing circuit is further adapted to cause a host response signal received by the receiving circuit, and which is only transmitted if the ID code signal matches an ID code stored at the host system, to be encrypted according to an encryption algorithm employing the personal encryption key and to cause the encrypted host response signal to be transmitted by the transmitting circuit only if the fingerprint signal corresponds sufficiently to the fingerprint template to verify that the user is an enrolled person.

23. The personal identification device of claim 22, further comprising an alphanumeric display.

24. The personal identification device of claim 23, further comprising a keypad for inputting data.

25. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the biometric trait;

a processing unit responsive to the biometric signal, being adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and

a communication unit, including a transmitter circuit, adapted to transmit the verification signal and an ID code signal to a remote host system associated with the host facility, wherein the ID code signal is indicative of an ID code associated only with the portable device, and wherein the host system provides access to the host facility in response to the verification signal only if host system determines that the personal device associated with the ID code belongs to a registered person.

26. A method of accessing a secure host facility, comprising:

sensing a biometric trait of a user that is unique to the user with a biometric sensor system of a portable device, and providing a biometric signal indicative of the biometric trait;

comparing, with the portable device, the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person;

providing a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person;

encrypting the verification signal;

wirelessly transmitting the encrypted verification signal and an ID code signal to a remote host system associated with the host facility, wherein the ID code signal is indicative of an ID code associated only with the portable device;

decrypting the encrypted verification signal only if the personal device associated with the ID code belongs to a registered person; and

providing access to their host facility only if certain verification information in the decrypted verification signal matches information stored at the host system.

27. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the biometric trait;

a processing unit responsive to the biometric signal, being adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person, and to provide an encrypted verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and

a communication unit, including a transmitter circuit, adapted to wirelessly transmit the encrypted verification signal and an ID code signal to a remote host system associated with the host facility, wherein the ID code signal is indicative of an ID code associated only with the portable hand-held device, and wherein the host system decrypts the encrypted verification signal only if the host system determines that the portable hand-held device associated with the ID code belongs to a registered person and provides access to the host facility only if certain verification information in the decrypted verification signal matches verification information stored at the host system.

* * * * *